FortiAnalyzer - CLI Reference

Version 6.0.3

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

November 02, 2018
FortiAnalyzer 6.0.3 CLI Reference
05-603-472611-20181102

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-11-02	Initial release.

Introduction

FortiAnalyzer offers centralized network security logging and reporting for the Fortinet Security Fabric. It provides a consolidated view across Fortinet devices throughout your organization with real-time alerts that expedite the discovery, investigation, and response to incidents even as they're happening. With action-oriented views and deep drill-down capabilities, FortiAnalyzer gives organizations critical insight into threats across the entire attack surface. It also provides real-time threat intelligence and actionable analytics via global IOC feeds to check for emerging and recent threats throughout the organization.

FortiAnalyzer includes:

- Centralized logging, reporting and event correlation
- Powerful NOC/SOC dashboard
- Automated indicators of compromise (IOC)
- Real-time and historical views into network activity

FortiAnalyzer documentation

The following FortiAnalyzer product documentation is available:

- *FortiAnalyzer Administration Guide*
  This document describes how to set up the FortiAnalyzer system and use it with supported Fortinet units.
- *FortiAnalyzer device QuickStart Guides*
  These documents are included with your FortiAnalyzer system package. Use this document to install and begin working with the FortiAnalyzer system and FortiAnalyzer GUI.
- *FortiAnalyzer Online Help*
  You can get online help from the FortiAnalyzer GUI. FortiAnalyzer online help contains detailed procedures for using the FortiAnalyzer GUI to configure and manage FortiGate units.
- *FortiAnalyzer CLI Reference*
  This document describes how to use the FortiAnalyzer Command Line Interface (CLI) and contains references for all FortiAnalyzer CLI commands.
- *FortiAnalyzer Release Notes*
  This document describes new features and enhancements in the FortiAnalyzer system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.
- *FortiAnalyzer VM Install Guide*
  This document describes installing FortiAnalyzer VM in your virtual environment.

What's New in FortiAnalyzer 6.0

The following tables list the commands and variables that have changed in the CLI.

FortiAnalyzer version 6.0.3

The table below lists commands that have changed in version 6.0.3.

Command	Change
`config fmupdate fds-setting`	Variable added: • fds-clt-ssl-protocol Variable removed: • fds-pull-interval Command added: • update-schedule
`config system admin profile`	Variables added: • adom-lock • device-policy-package-lock
`config system admin user`	Variables renamed: • radius-accprofile-override > ext-auth-accprofile-override • radius-adom-override > ext-auth-adom-override • radius-group-match > ext-auth-group-match
`config system global`	Variable removed: • admin-https-pki-required
`diagnose debug application`	Command removed: • vmtools Command added: • vmd
`diagnose system geoip-city`	Command added
`execute lvm extend`	Arguments removed

FortiAnalyzer version 6.0.2

The table below lists commands that have changed in version 6.0.2.

Command	Change
`config system admin profile`	Variable added: • datamask-custom-priority
`config system admin profile` `config datamask-custom-fields`	Variable added: • field-status
`config system global`	Variable added: • ssl-static-key-ciphers
`config system ha`	Command added: • preferred-role
`config system log-forward`	Variables added: • proxy-service • proxy-service-priority
`config system log settings`	Variable added: • FPX-custom-field1
`diagnose debug application faznotify`	Command added
`diagnose ha restart-init-sync`	Command added
`diagnose sql config report-engine set gen1`	Command removed
`diagnose test application faznotify`	Command added
`execute sql-report`	Commands added: • delete-font • delete-lang • export-lang Command updated: • list-lang Command removed: • del-font

FortiAnalyzer version 6.0.1

The table below lists commands that have changed in version 6.0.1.

Command	Change
`config fmupdate av-ips update-schedule`	Command removed
`config fmupdate web-spam fgd-setting`	Variable added: • fgd-pull-interval
`config fmupdate web-spam poll-frequency`	Command removed
`config system admin ldap`	Variables added:

Command	Change
	• memberof-attr • profile-attr • adom-attr
`config system admin profile`	Variables added: • datamask • datamask-fields • datamask-key Command added: • datamask-custom-fields
`config system admin setting`	Variable added: • objects-force-deletion
`config system admin user`	Variable added: • dev-group
`config system locallog {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting`	Variable added: • reliable
`diagnose dvm remove unused-ips-packages`	Command added
`diagnose fmupdate fds-dump-fmgi`	Command added
`diagnose sql hcache list`	Variable added: • max-time-scale
`execute reset hitcount`	Command added

FortiAnalyzer version 6.0.0

The table below lists commands that have changed in version 6.0.0.

Command	Change
`config fmupdate av-ips`	Commands removed: • fct • fgt
`config fmupdate fds-setting`	Command added: • server-override Variables added: • send_report • send_setup
`config fmupdate web-spam`	Commands removed: • fct • fgt • fsa

Command	Change
`config fmupdate web-spam fgd-setting server-override`	Command added
`config system admin setting`	Variable added: • show-hostname
`config system global`	Variables added: • hitcount_concurrent • hitcount_interval
`config system ha`	Command added
`config system locallog [memory | disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | syslogd | syslogd2 | syslogd3] filter`	Variables added: • diskquota • ediscovery • eventmgmt • fazha • fazsys • fortiview • hcache • logdb • logdev • logfile • logging • report
`config system log`	Command added: • ioc Command removed: • breach-detect
`config system log-forward`	Variable added: • fwd-secure
`config system report setting`	Variable added: • template-auto-install
`diagnose cdb upgrade pending-list`	Command added
`diagnose debug application`	Commands added: • apiproxyd • syncsched
`diagnose debug klog`	Command added
`diagnose dvm extender get-extender-modem-ip`	Command removed
`diagnose ha`	Command added
`diagnose log device`	Command updated
`diagnose sql config hcache-base-trim-interval`	Command added

Command	Change
`diagnose test application`	Commands added: • apiproxyd • syncsched
`execute certificate local import-pkcs12`	Command added
`execute sql-report`	Commands added: • delete-template • export-template • import-template • install-template • list-template

Using the Command Line Interface

This chapter explains how to connect to the CLI and describes the basics of using the CLI. You can use CLI commands to view all system information and to change all system configuration settings.

This chapter describes:

CLI command syntax

This guide uses the following conventions to describe command syntax.

- Angle brackets < > indicate variables.
- Vertical bar and curly brackets `{ | }` separate alternative, mutually exclusive required keywords.
  For example:
  ```
  set protocol {ftp | sftp}
  ```
  You can enter `set protocol ftp` or `set protocol sftp`.
- Square brackets `[ ]` indicate that a variable is optional.
  For example:
  ```
  show system interface [<name_str>]
  ```
  To show the settings for all interfaces, you can enter `show system interface`. To show the settings for the Port1 interface, you can enter `show system interface port1`.
- A space separates options that can be entered in any combination and must be separated by spaces.
  For example:
  ```
  set allowaccess {https ping}
  ```
  You can enter any of the following:
  ```
  set allowaccess ping
  set allowaccess https ping
  set allowaccess http https ping snmp ssh telnet webservice
  ```
  In most cases to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.
- Special characters:
  - The \ is supported to escape spaces or as a line continuation character.
  - The single quotation mark ' and the double quotation mark " are supported, but must be used in pairs.
  - If there are spaces in a string, you must precede the spaces with the \ escape character or put the string in a pair of quotation marks.

Connecting to the CLI

You can use a direct console connection, SSH, or the CLI console widget in the GUI to connect to the FortiAnalyzer CLI. For more information, see the FortiAnalyzer Administration Guide and your device's QuickStart Guide.

- Connecting to the FortiAnalyzer console
- Setting administrative access on an interface
- Connecting to the FortiAnalyzer CLI using SSH
- Connecting to the FortiAnalyzer CLI using the GUI

Connecting to the FortiAnalyzer console

To connect to the FortiAnalyzer console, you need:

- a computer with an available communications port
- a console cable, provided with your FortiAnalyzer unit, to connect the FortiAnalyzer console port to a communications port on your computer
- terminal emulation software, such as HyperTerminal for Windows.

The following procedure describes how to connect to the FortiAnalyzer CLI using Windows HyperTerminal software. You can use any terminal emulation program.

To connect to the CLI:

1. Connect the FortiAnalyzer console port to the available communications port on your computer.
2. Make sure that the FortiAnalyzer unit is powered on.
3. Start a terminal emulation program on the management computer, select the COM port, and use the following settings:

COM port	**COM1**
Baud rate	**9600**
Data bits	**8**
Parity	**None**
Stop bits	**1**
Flow control	**None**

4. Press `Enter` to connect to the FortiAnalyzer CLI.
5. In the log in prompt, enter the username and password.
   The default log in is username: `admin`, and no password.

   You have connected to the FortiAnalyzer CLI, and you can enter CLI commands.

Setting administrative access on an interface

To perform administrative functions through a FortiAnalyzer network interface, you must enable the required types of administrative access on the interface to which your management computer connects. Access to the CLI requires Secure Shell (SSH) access. If you want to use the GUI, you need HTTPS access.

To use the GUI to configure FortiAnalyzer interfaces for SSH access, see the FortiAnalyzer Administration Guide.

To use the CLI to configure SSH access:

1. Connect and log into the CLI using the FortiAnalyzer console port and your terminal emulation software.
2. Use the following command to configure an interface to accept SSH connections:
   ```
   config system interface
      edit <interface_name>
         set allowaccess <access_types>
      end
   ```
   Where `<interface_name>` is the name of the FortiAnalyzer interface to be configured to allow administrative access, and `<access_types>` is a whitespace-separated list of access types to enable.

   For example, to configure port1 to accept HTTPS and SSH connections, enter:
   ```
   config system interface
      edit port1
         set allowaccess https ssh
      end
   ```

   

   Remember to press `Enter` at the end of each line in the command example. Also, type `end` and press `Enter` to commit the changes to the FortiAnalyzer configuration.
3. To confirm that you have configured SSH access correctly, enter the following command to view the access settings for the interface:
   ```
   get system interface <interface_name>
   ```
   The CLI displays the settings, including the management access settings, for the named interface.

Connecting to the FortiAnalyzer CLI using SSH

SSH provides strong secure authentication and secure communications to the FortiAnalyzer CLI from your internal network or the internet. Once the FortiAnalyzer unit is configured to accept SSH connections, you can run an SSH client on your management computer and use this client to connect to the FortiAnalyzer CLI.

To connect to the CLI using SSH:

1. Install and start an SSH client.
2. Connect to a FortiAnalyzer interface that is configured for SSH connections.
3. Type a valid administrator name and press `Enter`.
4. Type the password for this administrator and press `Enter`.
   The FortiAnalyzer model name followed by a `#` is displayed.

   You have connected to the FortiAnalyzer CLI, and you can enter CLI commands.

Connecting to the FortiAnalyzer CLI using the GUI

The GUI also provides a CLI console window.

To connect to the CLI using the GUI:

1. Connect to the GUI and log in.
   For information about how to do this, see the FortiAnalyzer Administration Guide.
2. Go to *System Settings* > *Dashboard*.
3. Click inside the CLI Console widget. If the widget is not available, select *Toggle Widgets* from the toolbar to add the widget to the dashboard.

CLI objects

The FortiAnalyzer CLI is based on configurable objects. The top-level object are the basic components of FortiAnalyzer functionality.

system	Configuration options related to the overall operation of the FortiAnalyzer unit, such as interfaces, virtual domains, and administrators.
fmupdate	Configures settings related to FortiGuard service updates and the unit's built-in FDS.

This object contains more specific lower level objects. For example, the system object contains objects for administrators, DNS, interfaces and so on.

CLI command branches

The FortiAnalyzer CLI consists of the following command branches:

config branch	execute branch
get branch	diagnose branch
show branch	

Examples showing how to enter command sequences within each branch are provided in the following sections.

config branch

The `config` commands configure objects of FortiAnalyzer functionality. Top-level objects are not configurable, they are containers for more specific lower level objects. For example, the system object contains administrators, DNS addresses, interfaces, routes, and so on. When these objects have multiple sub-objects, such as administrators or routes, they are organized in the form of a table. You can add, delete, or edit the entries in the table. Table entries each consist of variables that you can set to particular values. Simpler objects, such as system DNS, are a single set of variables.

To configure an object, you use the `config` command to navigate to the object's command "shell". For example, to configure administrators, you enter the command

```
config system admin user
```

The command prompt changes to show that you are in the admin shell.

```
(user)#
```

This is a table shell. You can use any of the following commands:

edit	Add an entry to the FortiAnalyzer configuration or edit an existing entry. For example in the `config system admin` shell: • Type `edit admin` and press `Enter` to edit the settings for the default admin administrator account. • Type `edit newadmin` and press `Enter` to create a new administrator account with the name `newadmin` and to edit the default settings for the new administrator account.
delete	Remove an entry from the FortiAnalyzer configuration. For example in the `config system admin` shell, type `delete newadmin` and press `Enter` to delete the administrator account named `newadmin`.
purge	Remove all entries configured in the current shell. For example in the `config user local` shell: • Type `get` to see the list of user names added to the FortiAnalyzer configuration, • Type `purge` and then `y` to confirm that you want to purge all the user names, • Type `get` again to confirm that no user names are displayed.
get	List the configuration. In a table shell, `get` lists the table members. In an edit shell, `get` lists the variables and their values.
show	Show changes to the default configuration as configuration commands.
end	Save the changes you have made in the current shell and leave the shell. Every `config` command must be paired with an `end` command. You will return to the root FortiAnalyzer CLI prompt. The `end` command is also used to save `set` command changes and leave the shell.

If you enter the `get` command, you see a list of the entries in the table of administrators. To add a new administrator, you enter the edit command with a new administrator name:

```
edit admin_1
```

The FortiAnalyzer unit acknowledges the new table entry and changes the command prompt to show that you are now editing the new entry:

```
new entry 'admin_1' added
(admin_1)#
```

From this prompt, you can use any of the following commands:

config	In a few cases, there are subcommands that you access using a second config command while editing a table entry. An example of this is the command to add restrict the user to specific devices or VDOMs.
set	Assign values. For example from the `edit admin` command shell, typing `set password newpass` changes the password of the admin administrator account to `newpass`.

	When using a set command to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.
unset	Reset values to defaults. For example from the `edit admin` command shell, typing `unset password` resets the password of the admin administrator account to the default of no password.
get	List the configuration. In a table shell, `get` lists the table members. In an edit shell, `get` lists the variables and their values.
show	Show changes to the default configuration in the form of configuration commands.
next	Save the changes you have made in the current shell and continue working in the shell. For example if you want to add several new admin user accounts enter the `config system admin user` shell. • Type `edit User1` and press `Enter`. • Use the `set` commands to configure the values for the new admin account. • Type `next` to save the configuration for User1 without leaving the `config system admin user` shell. • Continue using the `edit`, `set`, and `next` commands to continue adding admin user accounts. • Type `end` and press `Enter` to save the last configuration and leave the shell.
abort	Exit an edit shell without saving the configuration.
end	Save the changes you have made in the current shell and leave the shell. Every `config` command must be paired with an `end` command. The `end` command is also used to save `set` command changes and leave the shell.

The `config` branch is organized into configuration shells. You can complete and save the configuration within each shell for that shell, or you can leave the shell without saving the configuration. You can only use the configuration commands for the shell that you are working in. To use the configuration commands for another shell you must leave the shell you are working in and enter the other shell.

get branch

Use `get` to display settings. You can use `get` within a `config` shell to display the settings for that shell, or you can use `get` with a full path to display the settings for the specified shell.

To use `get` from the root prompt, you must include a path to a shell.

The root prompt is the FortiAnalyzer host or model name followed by a number sign (#).

Example 1

When you type `get` in the `config system admin user` shell, the list of administrators is displayed.

At the `(user)#` prompt, type:

```
get
```

The screen displays:

```
== [ admin ]
userid: admin
```

```
== [ admin2 ]
userid: admin2
== [ admin3 ]
userid: admin3
```

Example 2

When you type `get` in the `admin` user shell, the configuration values for the admin administrator account are displayed.

```
edit admin
```

At the `(admin)#` prompt, type:

```
get
```

The screen displays:

```
userid : admin
password : *
trusthost1 : 0.0.0.0 0.0.0.0
trusthost2 : 0.0.0.0 0.0.0.0
trusthost3 : 0.0.0.0 0.0.0.0
trusthost4 : 0.0.0.0 0.0.0.0
trusthost5 : 0.0.0.0 0.0.0.0
trusthost6 : 0.0.0.0 0.0.0.0
trusthost7 : 0.0.0.0 0.0.0.0
trusthost8 : 0.0.0.0 0.0.0.0
trusthost9 : 0.0.0.0 0.0.0.0
trusthost10 : 127.0.0.1 255.255.255.255
ipv6_trusthost1 : ::/0
ipv6_trusthost2 : ::/0
ipv6_trusthost3 : ::/0
ipv6_trusthost4 : ::/0
ipv6_trusthost5 : ::/0
ipv6_trusthost6 : ::/0
ipv6_trusthost7 : ::/0
ipv6_trusthost8 : ::/0
ipv6_trusthost9 : ::/0
ipv6_trusthost10 : ::1/128
profileid : Super_User
adom:
   == [ all_adoms ]
   adom-name: all_adoms
policy-package:
   == [ all_policy_packages ]
   policy-package-name: all_policy_packages
restrict-access : disable
restrict-dev-vdom:
description : (null)
user_type : local
ssh-public-key1 :
ssh-public-key2 :
ssh-public-key3 :
meta-data:
last-name : (null)
first-name : (null)
email-address : (null)
phone-number : (null)
```

```
mobile-number : (null)
pager-number : (null)
hidden : 0
dashboard-tabs:
dashboard:
   == [ 6 ]
   moduleid: 6
   == [ 1 ]
   moduleid: 1
   == [ 2 ]
   moduleid: 2
   == [ 3 ]
   moduleid: 3
   == [ 4 ]
   moduleid: 4
   == [ 5 ]
   moduleid: 5
```

Example 3

You want to confirm the IP address and netmask of the port1 interface from the root prompt.

At the (command) # prompt, type:

```
get system interface port1
```

The screen displays:

```
name : port1
status : up
ip : 172.16.81.30 255.255.255.0
allowaccess : ping https ssh snmp telnet http webservice aggregator
serviceaccess :
speed : auto
description : (null)
alias : (null)
ipv6:
   ip6-address: ::/0 ip6-allowaccess:
```

show branch

Use `show` to display the FortiAnalyzer unit configuration. Only changes to the default configuration are displayed. You can use `show` within a `config` shell to display the configuration of that shell, or you can use `show` with a full path to display the configuration of the specified shell.

To display the configuration of all `config` shells, you can use `show` from the root prompt. The root prompt is the FortiAnalyzer host or model name followed by a number sign (#).

Example 1

When you type `show` and press `Enter` within the `port1` interface shell, the changes to the default interface configuration are displayed.

At the `(port1)` # prompt, type:

```
show
```

The screen displays:

```
config system interface
   edit "port1"
      set ip 172.16.81.30 255.255.255.0
      set allowaccess ping https ssh snmp telnet http webservice aggregator
   next
   edit "port2"
      set ip 1.1.1.1 255.255.255.0
      set allowaccess ping https ssh snmp telnet http webservice aggregator
   next
   edit "port3"
   next
   edit "port4"
   next
end
```

Example 2

You are working in the `port1` interface shell and want to see the `system dns` configuration. At the `(port1)#` prompt, type:

```
show system dns
```

The screen displays:

```
config system dns
   set primary 65.39.139.53
   set secondary 65.39.139.63
end
```

execute branch

Use `execute` to run static commands, to reset the FortiAnalyzer unit to factory defaults, or to back up or restore the FortiAnalyzer configuration. The execute commands are available only from the root prompt.

The root prompt is the FortiAnalyzer host or model name followed by a number sign (#).

Example

At the root prompt, type:

```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n)
```

and press `Enter` to restart the FortiAnalyzer unit.

diagnose branch

Commands in the `diagnose` branch are used for debugging the operation of the FortiAnalyzer unit and to set parameters for displaying different levels of diagnostic information.

Diagnose commands are intended for advanced users only. Contact Fortinet Technical Support before using these commands.

Example command sequences

The command prompt changes for each shell.

To configure the primary and secondary DNS server addresses:

1. Starting at the root prompt, type:
   ```
   config system dns
   ```
   and press `Enter`. The prompt changes to `(dns)#`.
2. At the `(dns)#` prompt, type (question mark) `?`
   The following options are displayed.
   ```
   set
   unset
   get
   show
   abort
   end
   ```
3. Type `set (question mark)?`
   The following options are displayed:
   ```
   primary
   secondary
   ```
4. To set the primary DNS server address to `172.16.100.100`, type:
   ```
   set primary 172.16.100.100
   ```
   and press `Enter`.
5. To set the secondary DNS server address to `207.104.200.1`, type:
   ```
   set secondary 207.104.200.1
   ```
   and press `Enter`.
6. To restore the primary DNS server address to the default address, type `unset primary` and press `Enter`.
7. If you want to leave the `config system dns` shell without saving your changes, type `abort` and press `Enter`.
8. To save your changes and exit the `dns` sub-shell, type `end` and press `Enter`.
9. To confirm your changes have taken effect after leaving the `dns` sub-shell, type `get system dns` and press `Enter`.

CLI basics

This section covers command line interface basic information.

Command help

You can press the question mark (?) key to display command help.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.
- Enter a command followed by a space and press the question mark (?) key to display a list of the options available for that command and a description of each option.
- Enter a command followed by an option and press the question mark (?) key to display a list of additional options available for that command option combination and a description of each option.

Command tree

Enter `tree` to display the FortiAnalyzer CLI command tree. To capture the full output, connect to your device using a terminal emulation program, such as PuTTY, and capture the output to a log file. For `config` commands, use the `tree` command to view all available variables and sub-commands.

Command completion

You can use the tab key or the question mark (?) key to complete commands.

- You can press the tab key at any prompt to scroll through the options available for that prompt.
- You can type the first characters of any command and press the tab key or the question mark (?) key to complete the command or to scroll through the options that are available at the current cursor position.
- After completing the first word of a command, you can press the space bar and then the tab key to scroll through the options available at the current cursor position.

Recalling commands

You can recall previously entered commands by using the Up and Down arrow keys to scroll through commands you have entered.

Editing commands

Use the left and right arrow keys to move the cursor back and forth in a recalled command. You can also use Backspace and Delete keys, and the control keys listed in the following table to edit the command.

Function	Key combination
Beginning of line	Control key + A
End of line	Control key + E
Back one character	Control key + B
Forward one character	Control key + F
Delete current character	Control key + D

Function	Key combination
Previous command	Control key + P
Next command	Control key + N
Abort the command	Control key + C
If used at the root prompt, exit the CLI	Control key + C

Line continuation

To break a long command over multiple lines, use a \ at the end of each line.

Command abbreviation

You can abbreviate commands and command options to the smallest number of non-ambiguous characters. For example, the command `get system status` can be abbreviated to `g sy st`.

Environment variables

The FortiAnalyzer CLI supports several environment variables.

$USERFROM	The management access type (SSH, Telnet and so on) and the IPv4 address of the logged in administrator.
$USERNAME	The user account name of the logged in administrator.
$SerialNum	The serial number of the FortiAnalyzer unit.

Variable names are case sensitive. In the following example, when entering the variable, you can type `$` followed by a tab to auto-complete the variable to ensure that you have the exact spelling and case. Continue pressing tab until the variable you want to use is displayed.

```
config system global
   set hostname $SerialNum
end
```

Encrypted password support

After you enter a clear text password using the CLI, the FortiAnalyzer unit encrypts the password and stores it in the configuration file with the prefix ENC. For example:

```
show system admin user user1
config system admin user
   edit "user1"
      set password ENC
           UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMFc9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQ
           xskRcU3E9XqOit82PgScwzGzGuJ5a9f
      set profileid "Standard_User"
   next
```

```
end
```

It is also possible to enter an already encrypted password. For example, type:

```
config system admin
```

then press `Enter`.

Enter:

```
edit user1
```

then press `Enter`.

Enter:

```
set password ENC
     UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMFc9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQxskRc
     U3E9XqOit82PgScwzGzGuJ5a9f
```

then press `Enter`.

Enter:

```
end
```

then press `Enter`.

Entering spaces in strings

When a string value contains a space, do one of the following:

- Enclose the string in quotation marks, `"Security Administrator"`, for example.
- Enclose the string in single quotes, `'Security Administrator'`, for example.
- Use a backslash (“\”) preceding the space, `Security\ Administrator`, for example.

Entering quotation marks in strings

If you want to include a quotation mark, single quote, or apostrophe in a string, you must precede the character with a backslash character. To include a backslash, enter two backslashes.

Entering a question mark (?) in a string

If you want to include a question mark (?) in a string, you must precede the question mark with CTRL-V. Entering a question mark without first entering CTRL-V causes the CLI to display possible command completions, terminating the string.

International characters

The CLI supports international characters in strings.

Special characters

The characters <, >, (,), #, ’, and " are not permitted in most CLI fields, but you can use them in passwords. If you use the apostrophe (‘) or quote (") character, you must precede it with a backslash (\) character when entering it in the CLI `set` command.

IPv4 address formats

You can enter an IPv4 address and subnet using either dotted decimal or slash-bit format. For example you can type either:

```
set ip 192.168.1.1 255.255.255.0
```

or

```
set ip 192.168.1.1/24
```

The IPv4 address is displayed in the configuration file in dotted decimal format.

Changing the baud rate

Using `execute console baudrate`, you can change the default console connection baud rate.

Changing the default baud rate is not available on all models.

Debug log levels

The following table lists available debug log levels on your FortiAnalyzer.

0	Emergency	The system has become unusable.
1	Alert	Immediate action is required.
2	Critical	Functionality is affected.
3	Error	An erroneous condition exists and functionality is probably affected.
4	Warning	Function might be affected.
5	Notice	Notification of normal events.
6	Information	General information about system operations.
7	Debug	Detailed information useful for debugging purposes.
8	Maximum	Maximum log level.

Administrative Domains

Administrative domains (ADOMs) enable the admin administrator to constrain other Fortinet unit administrators' access privileges to a subset of devices in the device list. For FortiGate devices with virtual domains (VDOMs), ADOMs can further restrict access to only data from a specific FortiGate VDOM.

About ADOMs

Enabling ADOMs alters the structure and available functionality of the GUI and CLI according to whether you are logging in as the `admin` administrator, and, if you are not logging in as the `admin` administrator, the administrator account's assigned access profile.

The `admin` administrator can further restrict other administrators' access to specific configuration areas within their ADOM by using access profiles .

Characteristics of the CLI and GUI when ADOMs are enabled

	Admin administrator account	Other administrators
Access to config system global	Yes	No
Can create administrator accounts	Yes	No
Can enter all ADOMs	Yes	No

- If ADOMs are enabled and you log in as `admin`, a superset of the typical CLI commands appear, allowing unrestricted access and ADOM configuration.
  `config system global` contains settings used by the FortiAnalyzer unit itself and settings shared by ADOMs, such as the device list, RAID, and administrator accounts. It does not include ADOM-specific settings or data, such as logs and reports. When configuring other administrator accounts, an additional option appears allowing you to restrict other administrators to an ADOM.
- If ADOMs are enabled and you log in as any other administrator, you enter the ADOM assigned to your account. A subset of the typical menus or CLI commands appear, allowing access only to only logs, reports, quarantine files, content archives, IP aliases, and LDAP queries specific to your ADOM. You cannot access Global Configuration, or enter other ADOMs.
  By default, administrator accounts other than the `admin` account are assigned to the `root` ADOM, which includes all devices in the device list. By creating ADOMs that contain a subset of devices in the device list, and assigning them to administrator accounts, you can restrict other administrator accounts to a subset of the FortiAnalyzer unit's total devices or VDOMs.

The `admin` administrator account cannot be restricted to an ADOM. Other administrators are restricted to their ADOM, and cannot configure ADOMs or Global Configuration.

The maximum number of ADOMs varies by FortiAnalyzer model.

FortiAnalyzer Model	Maximum ADOMs
FAZ-100C	100
FAZ-200D	150
FAZ-300D	175
FAZ-400C	300
FAZ-1000C, and FAZ-1000D	2 000
FAZ-3000D and FAZ-3000E	2 000
FAZ-3500E and FAZ-3900E	4 000
FAZ-4000B	2 000
FAZ-VM32 and FAZ-VM64	10 000

Configuring ADOMs

To use administrative domains, the `admin` administrator must first enable the feature, create ADOMs, and assign existing FortiAnalyzer administrators to ADOMs.

Enabling ADOMs moves non-global configuration items to the `root` ADOM. Back up the FortiAnalyzer unit configuration before enabling ADOMs.

Within the CLI, you can enable ADOMs and set the administrator ADOM. To configure the ADOMs, you must use the GUI.

To enable or disable ADOMs:

Enter the following CLI command:

```
config system global
   set adom-status {enable | disable}
end
```

An administrative domain has two modes: normal and advanced. Normal mode is the default device mode. In normal mode, a FortiGate unit can only be added to a single administrative domain. In advanced mode, you can assign different VDOMs from the same FortiGate to multiple administrative domains.

Enabling the advanced mode option will result in more complicated management scenarios. It is recommended only for advanced users.

To change ADOM device modes:

Enter the following CLI command:

```
config system global
   set adom-mode {advanced | normal}
end
```

To assign an administrator to an ADOM:

Enter the following CLI command:

```
config system admin user
   edit <name>
      set adom <adom_name>
   next
end
```

where <name> is the administrator user name and <adom_name> is the ADOM name.

system

Use system commands to configure options related to the overall operation of the FortiAnalyzer unit.

FortiAnalyzer CLI commands and variables are case sensitive.

admin

Use the following commands to configure admin related settings.

admin group

Use this command to add, edit, and delete admin user groups.

Syntax

```
config system admin group
   edit <name>
      set member <string>
end
```

Variable	Description
<name>	Enter the name of the group you are editing or enter a new name to create an entry (character limit = 63).
member <string>	Add group members.

admin ldap

Use this command to add, edit, and delete Lightweight Directory Access Protocol (LDAP) users.

Syntax

```
config system admin ldap
   edit <server>
      set adom-attr <string>
      set adom <adom-name>
      set attributes <filter>
      set ca-cert <string>
```

```
        set cnid <string>
        set connect-timeout <integer>
        set dn <string>
        set filter <string>
        set group <string>
        set memberof-attr <string>
        set password <passwd>
        set port <integer>
        set profile-attr <string>
        set secondary-server <string>
        set secure {disable | ldaps | starttls}
        set server <string>
        set tertiary-server <string>
        set type {anonymous | regular | simple}
        set username <string>
end
```

Variable	Description
<server>	Enter the name of the LDAP server or enter a new name to create an entry (character limit = 63).
adom-attr <string>	The attribute used to retrieve ADOM.
adom <adom-name>	Set the ADOM name to link to the LDAP configuration.
attributes <filter>	Attributes used for group searching (for multi-attributes, a use comma as a separator). For example: • `member` • `uniquemember` • `member,uniquemember`
ca-cert <string>	CA certificate name. This variable appears only when `secure` is set to `ldaps` or `starttls`.
cnid <string>	Enter the common name identifier (character limit = 20, default = cn).
connect-timeout <integer>	Set the LDAP connection timeout, in milliseconds (default = 500).
dn <string>	Enter the distinguished name.

filter <string>	Enter content for group searching. For example:
	`(&(objectcategory=group)(member=*))`
	`(&(objectclass=groupofnames)(member=*))`
	`(&(objectclass=groupofuniquenames)(uniquemember=*))`
	`(&(objectclass=posixgroup)(memberuid=*))`

group <string>	Enter an authorization group. The authentication user must be a member of this group (full DN) on the server.
memberof-attr <string>	The attribute used to retrieve memeberof.
password <passwd>	Enter a password for the username above. This variable appears only when `type` is set to `regular`.
port <integer>	Enter the port number for LDAP server communication (1 - 65535, default = 389).
profile-attr <string>	The attribute used to retrieve admin profile.

Variable	Description
secondary-server <string>	Enter the secondary LDAP server domain name or IPv4 address. Enter a new name to create a new entry.
secure {disable | ldaps | starttls}	Set the SSL connection type: • `disable`: no SSL (default). • `ldaps`: use LDAPS • `starttls`: use STARTTLS
server <string>	Enter the LDAP server domain name or IPv4 address. Enter a new name to create a new entry.
tertiary-server <string>	Enter the tertiary LDAP server domain name or IPv4 address. Enter a new name to create a new entry.
type {anonymous | regular | simple}	Set a binding type: • `anonymous`: Bind using anonymous user search • `regular`: Bind using username/password and then search • `simple`: Simple password authentication without search (default)
username <string>	Enter a username. This variable appears only when `type` is set to `regular`.

Example

This example shows how to add the LDAP user `user1` at the IPv4 address `206.205.204.203`.

```
config system admin ldap
   edit user1
      set server 206.205.204.203
      set dn techdoc
      set type regular
      set username auth1
      set password auth1_pwd
      set group techdoc
   end
```

admin profile

Use this command to configure access profiles. In a newly-created access profile, no access is enabled. Setting an option to `none` hides it from administrators with that profile assigned.

Syntax

```
config system admin profile
   edit <profile_name>
      set adom-lock {none | read | read-write}
      set adom-switch {none | read | read-write}
      set change-password {enable | disable}
      set datamask {enable | disable}
      set datamask-custom-priority {enable | disable}
      set datamask-fields <fields>
```

```
    set datamask-key <passwd>
    set description <text>
    set device-ap {none | read | read-write}
    set device-forticlient {none | read | read-write}
    set device-fortiswitch {none | read | read-write}
    set device-manager {none | read | read-write}
    set device-op {none | read | read-write}
    set device-policy-package-lock {none | read | read-write}
    set device-wan-link-load-balance {none | read | read-write}
    set event-management {none | read | read-write}
    set log-viewer {none | read | read-write}
    set realtime-monitor {none | read | read-write}
    set report-viewer {none | read | read-write}
    set scope {adom | global}
    set system-setting {none | read | read-write}
    config datamask-custom-fields
       edit <field>
          set field-category {alert | all | fortiview | log | euba}
          set field-status {enable | disable}
          set field-type {email | ip | mac | string}
       next
end
```

Variable	Description
<profile>	Edit the access profile. Enter a new name to create a new profile (character limit = 35). The pre-defined access profiles are *Super_User*, *Standard_User*, and *Restricted_User*.
adom-lock {none | read | read-write}	Configure ADOM locking permissions for profile: • `none`: No permission (default). • `read`: Read permission. • `read-write`: Read-write permission. Controlled functions: ADOM locking. Dependencies: `type` must be `system`
adom-switch {none | read | read-write}	Configure administrative domain (ADOM) permissions for this profile. Controlled functions: ADOM settings in DVM, ADOM settings in All ADOMs page (under System Settings tab) Dependencies: If `system-setting` is `none`, the All ADOMs page is not accessible.
change-password {enable | disable}	Enable/disable allowing restricted users to change their password (default = disable).
datamask {enable | disable}	Enable/disable data masking (default = disable).
datamask-custom-priority {enable | disable}	Enable/disable custom field search priority.
datamask-fields <fields>	Enter that data masking fields, separated by spaces. • *dstip*: Destination IP • *dstname*: Destination name • *email*: Email

Variable	Description
	• *message*: Message • *srcip*: Source IP • *srcmac*: Source MAC • *srcname*: Source name • *user*: User name
datamask-key <passwd>	Enter the data masking encryption key.
description <string>	Enter a description for this access profile (character limit = 1023). Enclose the description in quotes if it contains spaces.
device-ap {none | read | read-write}	Set the AP Manager permissions (default = none).
device-forticlient {none | read | read-write}	Set the FortiClient Manager permissions (default = none).
device-fortiswitch {none | read | read-write}	Set the FortiSwitch Manager permissions (default = none).
device-manager {none | read | read-write}	Enter the level of access to Device Manager settings for this profile (default = none). This command corresponds to the Device Manager option in the GUI administrator profile. Controlled functions: Device Manager
device-op {none | read | read-write}	Add the capability to add, delete, and edit devices to this profile (default = none). This command corresponds to the Add/Delete Devices/Groups option in the GUI administrator profile. This is a sub-setting of `device-manager`. Controlled functions: Add or delete devices or groups
device-policy-package-lock {none | read | read-write}	Configure device policy package locking permissions for this profile (default = none). Controlled functions: Policy package locking. Dependencies: `type` must be `system`
device-wan-link-load-balance {none | read | read-write}	Set the SD-WAN permissions (default = none).
event-management {none | read | read-write}	Set the Event Management permissions (default = none). This command corresponds to the Event Management option in the GUI administrator profile. Controlled functions: Event Management tab and all its operations
log-viewer {none | read | read-write}	Set the Log View permissions (default = none). This command corresponds to the Log View option in the GUI administrator profile. Controlled functions: Log View and all its operations

Variable	Description
realtime-monitor {none | read | read-write}	Enter the level of access to the Drill Down configuration settings for this profile (default = none).
report-viewer {none | read | read-write}	Set the Reports permissions (default = none). This command corresponds to the Reports option in the GUI administrator profile. Controlled functions: Reports tab and all its operations
scope (Not Applicable)	CLI command is not in use.
system-setting {none | read | read-write}	Configure System Settings permissions for this profile (default = none). This command corresponds to the System Settings option in the GUI administrator profile. Controlled functions: System Settings tab, All the settings under System setting
Variables for `config datamask-custom-fields` **subcommand**:	
<field>	Enter the custom field name.
field-category {alert | all | fortiview | log | euba}	Enter the field category (default = all).
field-status {enable | disable}	Enable/disable the field (default = enable).
field-type {email | ip | mac | string}	Enter the field type (default = string).

admin radius

Use this command to add, edit, and delete administration RADIUS servers.

Syntax

```
config system admin radius
   edit <server>
      set auth-type {any | chap | mschap2 | pap}
      set nas-ip <ipv4_address>
      set port <integer>
      set secondary-secret <passwd>
      set secondary-server <string>
      set secret <passwd>
      set server <string>
end
```

Variable	Description
<server>	Enter the name of the RADIUS server or enter a new name to create an entry (character limit = 63).
auth-type {any | chap | mschap2 | pap}	The authentication protocol the RADIUS server will use.

Variable	Description
	• any: Use any supported authentication protocol (default). • mschap2: Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2). • chap: Challenge Handshake Authentication Protocol (CHAP) • pap: Password Authentication Protocol (PAP).
nas-ip <ipv4_address>	The network access server (NAS) IPv4 address and called station ID.
port <integer>	The RADIUS server port number (1 - 65535 , default = 1812).
secondary-secret <passwd>	The password to access the RADIUS secondary-server (character limit = 64).
secondary-server <string>	The RADIUS secondary-server DNS resolvable domain name or IPv4 address.
secret <passwd>	The password to access the RADIUS server (character limit = 64).
server <string>	The RADIUS server DNS resolvable domain name or IPv4 address.

Example

This example shows how to add the RADIUS server RAID1 at the IPv4 address 206.205.204.203 and set the shared secret as R1a2D3i4U5s.

```
config system admin radius
   edit RAID1
      set server 206.205.204.203
      set secret R1a2D3i4U5s
   end
```

admin setting

Use this command to configure system administration settings, including web administration ports, timeout, and language.

Syntax

```
config system admin setting
   set access-banner {enable | disable}
   set admin-https-redirect {enable | disable}
   set admin-login-max <integer>
   set admin_server_cert <admin_server_certificate>
   set banner-message <string>
   set gui-them <theme>
   set http_port <integer>
   set https_port <integer>
   set idle_timeout <integer>
   set objects-force-deletion {enable | disable}
   set shell-access {enable | disable}
   set shell-password <passwd>
   set show-add-multiple {enable | disable}
   set show-checkbox-in-table {enable | disable}
```

```
    set show-device-import-export {enable | disable}
    set show_hostname {enable | disable}
    set show-log-forwarding {enable | disable}
    set unreg_dev_opt {add_allow_service | add_no_service}
    set webadmin_language {auto_detect | english | japanese | korean | simplified_chinese |
         traditional_chinese}
end
```

Variable	Description
access-banner {enable | disable}	Enable/disable the access banner (default= disable).
admin-https-redirect {enable | disable}	Enable/disable redirection of HTTP admin traffic to HTTPS (default= enable).
admin-login-max <integer>	Set the maximum number of admin users that be logged in at one time (1 - 256, default = 256).
admin_server_cert <admin_server_certificate>	Enter the name of an https server certificate to use for secure connections (default = server.crt). FortiAnalyzer has server.crt and Fortinet_Local certificates pre-loaded.
banner-message <string>	Set the banner messages (character limit = 255).
gui-theme <theme>	Configure the GUI theme (default = blue).
http_port <integer>	Enter the HTTP port number for web administration (1 - 65535, default = 80).
https_port <integer>	Enter the HTTPS port number for web administration (1 - 65535, default = 443).
idle_timeout <integer>	Enter the idle timeout value, in minutes (1 - 480, default = 15).
objects-force-deletion {enable | disable}	Enable/disable forced deletion of used objects (default = enable).
shell-access {enable | disable}	Enable/disable shell access (default = disable).
shell-password <passwd>	Enter the password to use for shell access.
show-add-multiple {enable | disable}	Enable/disable show the add multiple button in the GUI (default = disable).
show-checkbox-in-table {enable | disable}	Enable/disable show checkboxes in tables in the GUI (default = disable).
show-device-import-export {enable | disable}	Enable/disable import/export of ADOM, device, and group lists (default = disable).
show_hostname {enable | disable}	Enable/disable showing the hostname on the GUI login page (default = disable).
show-log-forwarding {enable | disable}	Enable/disable show log forwarding tab in analyzer mode (default= enable).
unreg_dev_opt {add_allow_service | add_no_service}	Select action to take when an unregistered device connects to FortiAnalyzer: • `add_allow_service`: Add unregistered devices and allow service requests (default). • `add_no_service`: Add unregistered devices and deny service requests.

Variable	Description
webadmin_language {auto_detect | english | japanese | korean | simplified_chinese | traditional_chinese}	Enter the language to be used for web administration. The following options are available: • auto_detect: Automatically detect language (default). • english: English. • japanese: Japanese. • korean: Korean. • simplified_chinese: Simplified Chinese. • traditional_chinese: Traditional Chinese.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system admin setting
```

admin tacacs

Use this command to add, edit, and delete administration TACACS+ servers.

Syntax

```
config system admin tacacs
   edit <server>
      set authen-type {ascii | auto |chap | mschap | pap}
      set authorization {enable | disable}
      set key <passwd>
      set port <integer>
      set secondary-key <passwd>
      set secondary-server <string>
      set server <string>
      set tertiary-key <passwd>
      set tertiary-server <string>
end
```

Variable	Description
<server>	Enter the name of the TACACS+ server or enter a new name to create an entry (character limit = 63).
authen-type {ascii | auto |chap | mschap | pap}	Choose which authentication type to use: • ascii: ASCII • auto: Uses PAP, MSCHAP, and CHAP (in that order) (default). • chap: Challenge Handshake Authentication Protocol (CHAP) • mschap: Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) • pap: Password Authentication Protocol (PAP).
authorization {enable | disable}	Enable/disable TACACS+ authorization (default = disable).
key <passwd>	Key to access the server (character limit = 128).

Variable	Description
port <integer>	Port number of the TACACS+ server (1 - 65535, default = 49).
secondary-key <passwd>	Key to access the secondary server (character limit = 128).
secondary-server <string>	Secondary server domain name or IPv4 address.
server <string>	The server domain name or IPv4 address.
tertiary-key <passwd>	Key to access the tertiary server (character limit = 128).
tertiary-server <string>	Tertiary server domain name or IPv4 address.

Example

This example shows how to add the TACACS+ server `TAC1` at the IPv4 address `206.205.204.203` and set the key as `R1a2D3i4U5s`.

```
config system admin tacacs
   edit TAC1
      set server 206.205.204.203
      set key R1a2D3i4U5s
   end
```

admin user

Use this command to add, edit, and delete administrator accounts.

Use the admin account or an account with System Settings read and write privileges to add new administrator accounts and control their permission levels. Each administrator account must include a minimum of an access profile. The access profile list is ordered alphabetically, capitals first. If custom profiles are defined, it may change the default profile from Restricted_User. You cannot delete the admin administrator account. You cannot delete an administrator account if that user is logged on.

You can create meta-data fields for administrator accounts. These objects must be created using the FortiAnalyzer GUI. The only information you can add to the object is the value of the field (pre-determined text/numbers). For more information, see *System Settings* in the *FortiAnalyzer Administration Guide*.

Syntax

```
config system admin user
   edit <name_str>
      set password <passwd>
      set change-password {enable | disable}
      set trusthost1 <ipv4_mask>
      set trusthost2 <ipv4_mask>
      set trusthost3 <ipv4_mask>
      ...
      set trusthost10 <ipv4_mask>
      set ipv6_trusthost1 <ipv6_mask>
```

```
set ipv6_trusthost2 <ipv6_mask>
set ipv6_trusthost3 <ipv6_mask>
...
set ipv6_trusthost10 <ipv6_mask>
set profileid <profile-name>
set adom <adom_name(s)>
set dev-group <group-name>
set adom-exclude <adom_name(s)>
set policy-package <policy-package-name>
set restrict-access {enable | disable}
set description <string>
set user_type {group | ldap | local | pki-auth | radius | tacacs-plus}
set group <string>
set ldap-server <string>
set radius_server <string>
set tacacs-plus-server <string>
set ssh-public-key1 <key-type> <key-value>
set ssh-public-key2 <key-type>, <key-value>
set ssh-public-key3 <key-type> <key-value>
set avatar <string>
set wildcard <enable | disable>
set ext-auth-accprofile-override <enable | disable>
set ext-auth-adom-override <enable | disable>
set ext-auth-group-match <string>
set password-expire <yyyy-mm-dd>
set force-password-change {enable | disable}
set subject <string>
set ca <string>
set two-factor-auth {enable | disable}
set rpc-permit {none | read-only | read-write}
set last-name <string>
set first-name <string>
set email-address <string>
set phone-number <string>
set mobile-number <string>
set pager-number <string>
config meta-data
   edit <fieldname>
      set fieldlength
      set fieldvalue <string>
      set importance
      set status
   end
config dashboard-tabs
   edit tabid <integer>
      set name <string>
   end
config dashboard
   edit moduleid
      set name <string>
      set column <column_pos>
      set diskio-content-type
      set diskio-period {1hour | 24hour | 8hour}
      set refresh-inverval <integer>
      set status {close | open}
      set tabid <integer>
      set widget-type <string>
```

```
            set log-rate-type {device | log}
            set log-rate-topn {1 | 2 | 3 | 4 | 5}
            set log-rate-period {1hour | 2min | 6hours}
            set res-view-type {history | real-time}
            set res-period {10min | day | hour}
            set res-cpu-display {average | each}
            set num-entries <integer>
            set time-period {1hour | 24hour | 8hour}
         end
      config restrict-dev-vdom
         edit dev-vdom <string>
      end
end
```

Variable	Description
<name_string>	Enter the name of the admin user or enter a new name to create a new user (character limit = 35).
password <passwd>	Enter a password for the administrator account (character limit = 128). For improved security, the password should be at least 6 characters long. This variable is available only if `user_type` is `local`.
change-password {enable | disable}	Enable/disable allowing restricted users to change their password (default = disable).
trusthost1 <ipv4_mask> trusthost2 <ipv4_mask> ... trusthost10 <ipv4_mask>	Optionally, type the trusted host IPv4 address and network mask from which the administrator can log in to the FortiAnalyzer system. You can specify up to ten trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. Defaults: `trusthost1`: `0.0.0.0 0.0.0.0` for all others: `255.255.255.255 255.255.255.255` for none
ipv6_trusthost1 <ipv6_mask> ipv6_trusthost2 <ipv6_mask> ... ipv6_trusthost10 <ipv6_mask>	Optionally, type the trusted host IPv6 address from which the administrator can log in to the FortiAnalyzer system. You can specify up to ten trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system. Defaults: `ipv6_trusthost1`: `::/0` for all others: `ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128` for none
profileid <profile-name>	Enter the name of the access profile to assign to this administrator account (character limit = 35, default = Restricted_User). Access profiles control administrator access to FortiAnalyzer features.
adom <adom_name(s)>	Enter the name(s) of the ADOM(s) the administrator belongs to. Any configuration of ADOMs takes place via the FortiAnalyzer GUI.
dev-group <group-name>	Enter the device group that the admin use can access. This option can only be used for administrators with access to only one ADOM.
adom-exclude <adom_name(s)>	Enter the name(s) of the excluding ADOM(s).

Variable	Description
policy-package {<adom name>: <policy package id> <adom policy folder name>/ <package name> | all_policy_ packages}	Policy package access
restrict-access {enable | disable}	Enable/disable restricted access to the development VDOM (`dev-vdom`) (default = disable).
description <string>	Enter a description for this administrator account (character limit = 127). Enclose the description in quotes if it contains spaces.
user_type {group | ldap | local | pki-auth | radius | tacacs-plus}	Select the administrator type: • `group`: The administratoris a member of a administrator group. • `ldap`: An LDAP server verifies the administrator's password. • `local`: The FortiAnalyzer system verifies the administrator's password (default). • `pki-auth`: The administrator uses PKI. • `radius`: A RADIUS server verifies the administrator's password. • `tacacs-plus`: A TACACS+ server verifies the administrator's password.
group <string>	Enter the group name.
ldap-server <string>	Enter the LDAP server name if the user type is set to LDAP.
radius_server <string>	Enter the RADIUS server name if the user type is set t o RADIUS.
tacacs-plus-server <string>	Enter the TACACS+ server name if the user type is set to TACACS+.
ssh-public-key1 <key-type> <key-value> ssh-public-key2 <key-type> <key-value> ssh-public-key3 <key-type> <key-value>	You can specify the public keys of up to three SSH clients. These clients are authenticated without being asked for the administrator password. You must create the public-private key pair in the SSH client application. `<key type>` is `ssh-dss` for a DSA key, `ssh-rsa` for an RSA key. `<key-value>` is the public key string of the SSH client.
avatar <string>	Image file for the administrator's avatar (maximum 4K base64 encode).
wildcard <enable | disable>	Enable/disable wildcard remote authentication (default = disable).
ext-auth-accprofile-override <enable | disable>	Enable/disable allowing the use of the access profile provided by the remote authentication server (default = disable).
ext-auth-adom-override <enable | disable>	Enable/disable allowing the use of the ADOM provided by the remote authentication server (default = disable). In order to support vendor specific attributes (VSA), the authentication server requires a dictionary to define which VSAs to support. The Fortinet RADIUS vendor ID is `12365`. The `Fortinet-Vdom-Name` attribute is used by this command.
ext-auth-group-match <string>	Only admin users that belong to this group are allowed to log in.

Variable	Description
password-expire <yyyy-mm-dd>	When enforcing the password policy, enter the date that the current password will expire.
force-password-change {enable | disable}	Enable/disable force password change on next log in.
subject <string>	PKI user certificate name constraints. This command is available when a PKI administrator account is configured.
ca <string>	PKI user certificate CA (CA name in local). This command is available when a PKI administrator account is configured.
two-factor-auth {enable | disable}	Enable/disable two-factor authentication (certificate + password) (default = disable). This command is available when a PKI administrator account is configured.
rpc-permit {none | read-only | read-write}	Set the permission level for log in via Remote Procedure Call (RPC) (default = none).
last-name <string>	Administrator's last name (character limit = 63).
first-name <string>	Administrator's first name (character limit = 63).
email-address <string>	Administrator's email address.
phone-number <string>	Administrator's phone number.
mobile-number <string>	Administrator's mobile phone number.
pager-number <string>	Administrator's pager number.
Variables for `config meta-data` **subcommand**: This subcommand can only change the value of an existing field. To create a new metadata field, use the `config system metadata` command.	
fieldname	The label/name of the field (read-only, default = 50). Enclose the name in quotes if it contains spaces.
fieldlength	The maximum number of characters allowed for this field (read-only, default = 50).
fieldvalue <string>	Enter a pre-determined value for the field. This is the only value that can be changed with the `config meta-data` subcommand (character limit = 255).
importance	Indicates whether the field is compulsory (`required`) or optional (`optional`) (read-only, default = optional).
status	The status of the field (read-only, default = enable).
Variables for `config dashboard-tabs` **subcommand**:	
tabid <integer>	Tab ID.
name <string>	Tab name.

Variable	Description
Variables for `config dashboard` **subcommand**:	
moduleid	Widget ID.
name <string>	Widget name (character limit = 63).
column <column_pos>	Widget column ID (default = 0).
diskio-content-type {blks | iops | util}	Set the Disk I/O Monitor widget's chart type. • `blks`: the amount of data of I/O requests. • `iops`: the number of I/O requests. • `util`: bandwidth utilization (default).
diskio-period {1hour | 24hour | 8hour}	Set the Disk I/O Monitor widget's data period (default = 1hour).
refresh-inverval <integer>	Widget refresh interval (default = 300).
status {close | open}	Widget opened/closed status (default = open).
tabid <integer>	ID of the tab where the widget is displayed (default = 0).
widget-type <string>	Widget type: • `alert`: Alert Message Console • `devsummary`: Device Summary • `disk-io`: Disk I/O • `jsconsole`: CLI Console • `licinfo`: License Information • `log-rcvd-fwd`Receive Rate v. Forwarding Rate • `logdb-lag`: Log Insert Lag Time • `logdb-perf`: Insert Rate vs Receive Rate • `logrecv`: Logs/Data Received (this widget has been deprecated) • `raid`: Disk Monitor • `rpteng`: Report Engine (this widget has been deprecated) • `statistics`: Statistics (this widget has been deprecated) • `sysinfo`: System Information • `sysop`: Unit Operation • `sysres`: System Resources • `top-lograte`: Log Receive Monitor
log-rate-type {device | log}	Log receive monitor widget’s statistics breakdown options (default = device).
log-rate-topn {1 | 2 | 3 | 4 | 5}	Log receive monitor widgets’s number of top items to display (default = 5).
log-rate-period {1hour | 2min | 6hours}	Log receive monitor widget’s data period (default = 2min).
res-view-type {history | real-time}	Widget’s data view type (default = history).
res-period {10min | day | hour}	Widget data period: • `10min`: Last 10 minutes (default). • `day`: Last day.

Variable	Description
	• `hour`: Last hour.
res-cpu-display {average | each}	Widget CPU display type: • `average`: Average usage of CPU (default). • `each`: Each usage of CPU.
num-entries <integer>	Number of entries (default = 10).
time-period {1hour | 24hour | 8hour}	Set the Log Database Monitor widget's data period (default = 1hour).
Variable for `config restrict-dev-vdom` **subcommand**:	
dev-vdom <string>	Enter device or VDOM to edit.

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IPv4 address if you define only one trusted host IPv4 address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiAnalyzer system does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply both to the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.

Example

Use the following commands to add a new administrator account named `admin_2` with the password set to `p8ssw0rd` and the `Super_User` access profile. Administrators that log in to this account will have administrator access to the FortiAnalyzer system from any IPv4 address.

```
config system admin user
   edit admin_2
      set description "Backup administrator"
      set password p8ssw0rd
      set profileid Super_User
   end
```

alert-console

Use this command to configure the alert console options. The alert console appears on the dashboard in the GUI.

Syntax

```
config system alert-console
   set period {1 | 2 | 3 | 4 | 5 | 6 | 7}
   set severity-level {information | notify | warning | error | critical | alert |
        emergency}
end
```

Variable	Description
period {1 | 2 | 3 | 4 | 5 | 6 | 7}	Enter the number of days to keep the alert console alerts (default = 7).
severity-level {information | notify | warning | error | critical | alert | emergency}	Enter the minimum severity level to display on the alert console on the dashboard: • `emergency`: The unit is unusable (default). • `alert`: Immediate action is required. • `critical`: Functionality is affected. • `error`: Functionality is probably affected. • `warning`: Functionality might be affected. • `notification`: Information about normal events. • `information`: General information about unit operations.

Example

This example sets the alert console message display to warning for a duration of three days.

```
config system alert-console
   set period 3
   set severity-level warning
end
```

alertemail

Use this command to configure alert email settings for your FortiAnalyzer unit.

All variables are required when `authentication` is enabled.

Syntax

```
config system alertemail
   set authentication {enable | disable}
   set fromaddress <email-address_string>
   set fromname <string>
   set smtppassword <passwd>
   set smtpport <integer>
   set smtpserver {<ipv4_address>|<fqdn_string>}
   set smtpuser <username>
end
```

Variable	Description
authentication {enable | disable}	Enable/disable alert email authentication (default = enable).
fromaddress <email-address_ string>	The email address the alert message is from. This is a required variable.
fromname <string>	The SMTP name associated with the email address. Enclose the name in quotes if it contains spaces.
smtppassword <passwd>	Set the SMTP server password (character limit = 39).
smtpport <integer>	The SMTP server port (1 - 65535, default = 25).
smtpserver {<ipv4_ address>|<fqdn_string>}	The SMTP server address, either a DNS resolvable host name or an IPv4 address.
smtpuser <username>	Set the SMTP server username (character limit= 63).

Example

Here is an example of configuring `alertemail`. Enable authentication, the alert is set in Mr. Customer's name and from his email address, the SMTP server port is the default port(25), and the SMTP server is at IPv4 address of 192.168.10.10.

```
config system alertemail
   set authentication enable
   set fromaddress customer@example.com
   set fromname "Ms. Customer"
   set smtpport 25
   set smtpserver 192.168.10.10
end
```

alert-event

Use `alert-event` commands to configure the FortiAnalyzer unit to monitor logs for log messages with certain severity levels, or information within the logs. If the message appears in the logs, the FortiAnalyzer unit sends an email or SNMP trap to a predefined recipient(s) of the log message encountered. Alert event messages provide immediate notification of issues occurring on the FortiAnalyzer unit.

When configuring an alert email, you must configure at least one DNS server. The FortiGate unit uses the SMTP server name to connect to the mail server and must look up this name on your DNS server.

`alert-event` was removed from the GUI in FortiAnalyzer version 5.0.3. This command has been kept in the CLI for customers who previously configured this function.

Syntax

```
config system alert-event
```

```
edit <name_string>
   set enable-generic-text {enable | disable}
   set enable-severity-filter {enable | disable}
   set event-time-period {0.5 | 1 | 3 | 6 | 12 | 24 | 72 | 168}
   set generic-text <string>
   set num-events {1 | 5 | 10 | 50 | 100}
   set severity-filter {high | low | medium | medium-high | medium-low}
   set severity-level-comp {>= | = | <=}
   set severity-level-logs {no-check | information | notify | warning |error | critical |
        alert | emergency}
   config alert-destination
      edit destination_id <integer>
         set type {mail | snmp | syslog}
         set from <email_address>
         set to <email_address>
         set smtp-name <server_name>
         set snmp-name <server_name>
         set syslog-name <server_name>
      end
end
```

Variable	Description
<name_string>	Enter a name for the alert event (character limit = 63).
enable-generic-text {enable | disable}	Enable generic text match (default = disable).
enable-severity-filter {enable | disable}	Enable/disable alert severity filter (default = disable).
event-time-period {0.5 | 1 | 3 | 6 | 12 | 24 | 72 | 168}	The period of time in hours during which if the threshold number is exceeded, the event will be reported: • 0.5: 30 minutes (default) • 1: 1 hour • 3: 3 hours • 6: 6 hours • 12: 12 hours • 24: 1 day • 72: 3 days • 168: 1 week
generic-text <string>	Text that must be contained in a log to trigger alert (character limit = 255).
num-events {1 | 5 | 10 | 50 | 100}	Set the minimum number of events that must occur in the given interval before it is reported (default = 1).
severity-filter {high | low | medium | medium-high | medium-low}	Set the required log severity to trigger an alert (default = high).
severity-level-comp {>= | = | <=}	Set the log severity threshold comparison criterion (default = =). Log messages are monitored based on the log level. For example, alerts may be monitored if the messages are greater than or equal to (>=) the Warning log level.

Variable	Description
severity-level-logs {no-check | information | notify | warning |error | critical | alert | emergency}	Set the log severity threshold level. That is, the log level the FortiManager looks for when monitoring for alert messages. • `no-check`: Do not check severity level for this log type (default). • `emergency`: The unit is unusable. • `alert`: Immediate action is required. • `critical`: Functionality is affected. • `error`: Functionality is probably affected. • `warning`: Functionality might be affected. • `notification`: Information about normal events. • `information`: General information about unit operations.
Variables for `config alert-destination` **subcommand**:	
destination_id <integer>	Enter the table sequence number, beginning at 1.
type {mail | snmp | syslog}	Select the alert event message method of delivery: • `mail`: Send email alert (default). • `snmp`: Send SNMP trap. • `syslog`: Send syslog message.
from <email_address>	Enter the sender email address to use in alert emails. This is available when `type` is set to `mail`.
to <email_address>	Enter the recipient email address to use in alert emails. This is available when `type` is set to `mail`.
smtp-name <server_name>	Enter the name of the mail server. This is available when `type` is set to `mail`.
snmp-name <server_name>	Enter the snmp server name. This is available when `type` is set to `snmp`.
syslog-name <server_name>	Enter the syslog server name or IPv4 address. This is available when `type` is set to `syslog`.

Example

In the following example, the alert message is set to send an email to the administrator when 5 warning log messages appear over the span of three hours.

```
config system alert-event
   edit warning
      config alert-destination
         edit 1
            set type mail
            set from fmgr@exmample.com
            set to admin@example.com
            set smtp-name mail.example.com
         end
         set enable-severity-filter enable
         set event-time-period 3
         set severity-level-log warning
         set severity-level-comp =
         set severity-filter medium
   end
```

auto-delete

Use this command to automatically delete policies for logs, reports, and archived and quarantined files.

Syntax

```
config system auto-delete
   config dlp-files-auto-deletion
      set retention {days | weeks | months}
      set runat <integer>
      set status {enable | disable}
      set value <integer>
   end
   config quarantine-files-auto-deletion
      set retention {days | weeks | months}
      set runat <integer>
      set status {enable | disable}
      set value <integer>
   end
   config log-auto-deletion
      set retention {days | weeks | months}
      set runat <integer>
      set status {enable | disable}
      set value <integer>
   end
   config report-auto-deletion
      set retention {days | weeks | months}
      set runat <integer>
      set status {enable | disable}
      set value <integer>
   end
end
```

Variable	Description
dlp-files-auto-deletion	Automatic deletion policy for DLP archives.
quarantine-files-auto-deletion	Automatic deletion policy for quarantined files.
log-auto-deletion	Automatic deletion policy for device logs.
report-auto-deletion	Automatic deletion policy for reports.
retention {days | weeks | months}	Automatic deletion in days, weeks, or months (default = days).
runat <integer>	Automatic deletion run at (0 - 23) o'clock (default = 0).
status {enable | disable}	Enable/disable automatic deletion (default = disable).
value <integer>	Automatic deletion in x days, weeks, or months (default = 0).

backup all-settings

Use this command to set or check the settings for scheduled backups.

Syntax

```
config system backup all-settings
   set status {enable | disable}
   set server {<ipv4_address>|<fqdn_str>}
   set user <username>
   set directory <string>
   set week_days {monday tuesday wednesday thursday friday saturday sunday}
   set time <hh:mm:ss>
   set protocol {ftp | scp | sftp}
   set passwd <passwd>
   set cert <string>
   set crptpasswd <passwd>
end
```

Variable	Description
status {enable | disable}	Enable/disable scheduled backups (default = disable).
server {<ipv4_address>|<fqdn_str>}	Enter the IPv4 address or DNS resolvable host name of the backup server.
user <username>	Enter the user account name for the backup server (character limit = 63).
directory <string>	Enter the name of the directory on the backup server in which to save the backup file.
week_days {monday tuesday wednesday thursday friday saturday sunday}	Enter the days of the week on which to perform backups. You may enter multiple days.
time <hh:mm:ss>	Enter the time of day to perform the backup. Time is required in the form <hh:mm:ss>.
protocol {ftp | scp | sftp}	Enter the transfer protocol (default = sftp).
passwd <passwd>	Enter the password for the backup server (character limit = 63).
cert <string>	SSH certificate for authentication. Only available if the protocol is set to scp.
crptpasswd <passwd>	Optional password to protect backup content (character limit = 63).

Example

This example shows a whack where backup server is 172.20.120.11 using the admin account with no password, saving to the `/usr/local/backup` directory. Backups are done on Mondays at 1:00pm using ftp.

```
config system backup all-settings
   set status enable
   set server 172.20.120.11
   set user admin
```

```
    set directory /usr/local/backup
    set week_days monday
    set time 13:00:00
    set protocol ftp
end
```

central-management

Use this command to set or check the settings for central management.

Syntax

```
config system central-management
    set type {fortimanager}
    set allow-monitor {enable | disable}
    set authorized-manager-only {enable | disable}
    set serial-number <serial_number_string>
    set fmg <string>
    set enc-alogorithm {default | high | low}
end
```

Variable	Description
type {fortimanager}	Type of management server (default = fortimanager).
allow-monitor {enable | disable}	Enable/disable remote monitoring of the device (default = enable).
authorized-manager-only {enable | disable}	Enable/disable restricted to authorize manager only setting (default = enable).
serial-number <serial_number_string>	Set the device serial number. You can enter up to 5 serial numbers.
fmg <string>	Set the IP address or FQDN of the FortiManager (character limit = 31).
enc-alogorithm {default | high | low}	Set the SSL communication encryption algorithms: • `default`: SSL communication with high and medium encryption algorithms (default) • `high`: SSL communication with high encryption algorithms • `low`: SSL communication with low encryption algorithms

Use the show command to display the current configuration if it has been changed from its default value:

```
show system central-management
```

certificate

Use the following commands to configure certificate related settings.

certificate ca

Use this command to install Certificate Authority (CA) root certificates.

When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA. he CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate. Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate ca
   edit <ca_name>
      set ca <certificate>
      set comment <string>
   end
```

Variable	Description
<ca_name>	Enter a name for the CA certificate (character limit = 35).
ca <certificate>	Enter or retrieve the CA certificate in PEM format.
comment <string>	Optionally, enter a descriptive comment (character limit = 127).

certificate crl

Use this command to configure CRLs.

Syntax

```
config system certificate crl
   edit <name>
      set crl <crl>
      set comment <string>
   end
```

Variable	Description
<name>	Enter a name for the CRL (character limit = 35).
crl <crl>	Enter or retrieve the CRL in PEM format.
comment <string>	Optionally, enter a descriptive comment for this CRL (character limit = 127).

certificate local

Use this command to install local certificates. When a CA processes your CSR, it sends you the CA certificate, the signed local certificate and the CRL.

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA. The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate. Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate local
   edit <cert_name>
      set password <passwd>
      set comment <string>
      set certificate <certificate_PEM>
      set private-key <prkey>
      set csr <csr_PEM>
   end
```

Variable	Description
<cert_name>	Enter the local certificate name (character limit = 35).
password <passwd>	Enter the local certificate password (character limit = 67).
comment <string>	Enter any relevant information about the certificate (character limit = 127).
certificate <certificate_PEM>	Enter the signed local certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit.	
private-key <prkey>	The private key in PEM format.
csr <csr_PEM>	The CSR in PEM format.

certificate oftp

Use this command to install OFTP certificates and keys.

Syntax

```
config system certificate oftp
      set certificate <certificate>
      set comment <string>
      set custom {enable | disable}
      set password <passwd>
      set private-key <key>
```

```
    end
```

Variable	Description
certificate <certificate>	PEM format certificate.
comment <string>	OFTP certificate comment (character limit = 127).
custom {enable | disable}	Enable/disable custom certificates (default = disable)..
password <passwd>	Password for encrypted 'private-key', unset for non-encrypted.
private-key <key>	PEM format private key.

certificate ssh

Use this command to install SSH certificates and keys.

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA. The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate.
5. Use the `system certificate SSH` command to install the SSH certificate. Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate ssh
   edit <name>
      set comment <comment_text>
      set certificate <certificate>
      set private-key <key>
   end
```

Variable	Description
<name>	Enter the SSH certificate name (character limit = 63).
comment <comment_text>	Enter any relevant information about the certificate (character limit = 127).
certificate <certificate>	Enter the signed SSH certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit.	
private-key <key>	The private key in PEM format.

dns

Use these commands to set the DNS server addresses. Several FortiAnalyzer functions, including sending alert email, use DNS. In FortiAnalyzer 5.2.1 or later, you can configure both IPv4 and IPv6 DNS server addresses.

Syntax

```
config system dns
   set primary <ipv4_address>
   set secondary <ipv4_address>
   set ip6-primary <ipv6_address>
   set ip6-secondary <ipv6_address>
end
```

Variable	Description
primary <ipv4_address>	Enter the primary DNS server IPv4 address.
secondary <ipv4_address>	Enter the secondary DNS IPv4 server address.
ip6-primary <ipv6_address>	Enter the primary DNS server IPv6 address.
ip6-secondary <ipv6_address>	Enter the secondary DNS IPv6 server address.

Example

This example shows how to set the primary FortiAnalyzer DNS server IPv4 address to `172.20.120.99` and the secondary FortiAnalyzer DNS server IPv4 address to `192.168.1.199`.

```
config system dns
   set primary 172.20.120.99
   set secondary 192.168.1.199
end
```

fips

Use this command to set the Federal Information Processing Standards (FIPS) status. FIPS mode is an enhanced security option for some FortiAnalyzer models. Installation of FIPS firmware is required only if the unit was not ordered with this firmware pre-installed.

Syntax

```
config system fips
   set status {enable | disable}
   set entropy-token {enable | disable | dynamic}
   set re-seed-interval <integer>
end
```

Variable	Description
status {enable | disable}	Enable/disable the FIPS-CC mode of operation (default = enable).
entropy-token {enable | disable | dynamic}	Configure support for the FortiTRNG entropy token when switching to FIPS mode: • `enable`: The token must be present during boot up and reseeding. If the token is not present, the boot up or reseeding is interrupted until the token is inserted. • `disable`: The current entropy implementation is used to seed the Random Number Generator (RNG) (default). • `dynamic`: The token is used to seed or reseed the RNG if it is present. If the token is not present, the boot process is not blocked and the old entropy implementation is used.
re-seed-interval <integer>	The amount of time between RNG reseeding, in minutes (0 - 1440, default = 1440).

fortiview

fortiview setting

Use this command to configure FortiView settings.

Syntax

```
config system fortiview setting
   set not-scanned apps {exclude | include}
   set resolve-ip {enable | disable}
end
```

Variable	Description
not-scanned apps {exclude | include}	Include/exclude unscanned applications in FortiView (default = include). Set to `exclude` to filter out never scanned applications.
resolve-ip {enable | disable}	Enable/disable resolving the IP address to the hostname in FortiView (default = disable).

fortiview auto-cache

Use this command to view or configure FortiView auto-cache settings.

Syntax

```
config system fortiview auto-cache
   set aggressive-fortiview {enable | disable}
```

```
    set interval <integer>
    set status {enable | disable}
end
```

Variable	Description
aggressive-fortiview {enable | disable}	Enable/disable aggressive auto-cache on FortiView (default = disable).
interval <integer>	The time interval for FortiView auto-cache, in hours (default = 168).
status {enable | disable}	Enable/disable FortiView auto-cache (default = enable).

global

Use this command to configure global settings that affect miscellaneous FortiAnalyzer features.

Syntax

```
config system global
   set admin-lockout-duration <integer>
   set admin-lockout-threshold <integer>
   set adom-mode {advanced | normal}
   set adom-select {enable | disable}
   set adom-status {enable | disable}
   set backup-compression {high | low | none | normal}
   set backup-to-subfolders {enable | disable}
   set clt-cert-req {enable | disable}
   set console-output {more | standard}
   set country-flag {enable | disable}
   set create-revision {enable | disable}
   set daylightsavetime {enable | disable}
   set default-disk-quota <integer>
   set default-search-mode {advanced | filter-based}
   set detect-unregistered-log-device {enable | disable}
   set device-view-mode {regular | tree}
   set enc-algorithm {high | medium | low}
   set fgfm-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
   set ha-member-auto-grouping {enable | disable}
   set hitcount_concurrent <integer>
   set hitcount_interval <integer>
   set hostname <string>
   set language {english | japanese | simch | trach}
   set ldap-cache-timeout <integer>
   set ldapconntimeout <integer>
   set lock-preempt {enable | disable}
   set log-checksum {md5 | md5-auth | none}
   set log-mode {analyzer | collector}
   set max-aggregation-tasks <integer>
   set max-log-forward <integer>
   set max-running-reports <integer>
   set oftp-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
   set policy-hit-count {enable | disable}
```

```
    set policy-object-in-dual-pane {enable | disable}
    set pre-login-banner {enable | disable}
    set pre-login-banner-message <string>
    set remoteauthtimeout <integer>
    set search-all-adoms {enable | disable}
    set ssl-low-encryption {enable | disable}
    set ssl-protocol {tlsv1.2 | tlsv1.1 | tlsv1.0 | sslv3}
    set ssl-static-key-ciphers {enable | disable}
    set task-list-size <integer>
    set tftp
    set timezone <integer>
    set tunnel-mtu <integer>
    set usg {enable | disable}
    set webservice-proto {tlsv1.2 | tlsv1.1 | tlsv1.0 | sslv3 | sslv2}
    set workflow-max-sessions <integer>
end
```

Variable	Description
admin-lockout-duration <integer>	Set the lockout duration for FortiAnalyzer administration, in seconds (default = 60).
admin-lockout-threshold <integer>	Set the lockout threshold for FortiAnalyzer administration (1 - 10, default = 3).
adom-mode {advanced | normal}	Set the ADOM mode (default = normal).
adom-select {enable | disable}	Enable/disable a pop-up window that allows administrators to select an ADOM after logging in (default = enable).
adom-status {enable | disable}	Enable/disable administrative domains (default = disable).
backup-compression {high | low | none | normal}	Set the backup compression level: `high` (slowest), `low` (fastest), `none`, or `normal` (default).
backup-to-subfolders {enable | disable}	Enable/disable the creation of subfolders on server for backup storage (default = disable).
clt-cert-req {enable | disable}	Enable/disable requiring a client certificate for GUI login (default = disable). When both `clt-cert-req` and `admin-https-pki-required` are enabled, only PKI administrators can connect to the GUI.
console-output {more | standard}	Select how the output is displayed on the console (default = standard). Select `more` to pause the output at each full screen until keypress. Select `standard` for continuous output without pauses.
country-flag {enable | disable}	Enable/disable a country flag icon beside an IP address (default = enable).
create-revision {enable | disable}	Enable/disable create revision by default (default = disable).
daylightsavetime {enable | disable}	Enable/disable daylight saving time (default = enable). If you enable daylight saving time, the FortiAnalyzer unit automatically adjusts the system time when daylight saving time begins or ends.
default-disk-quota <integer>	Default disk quota for registered device, in megabytes (100 - 100000, default = 1000).

Variable	Description
default-search-mode {advanced | filter-based}	Set the default search mode of log view (default = filter-based).
detect-unregistered-log-device {enable | disable}	Enable/disable unregistered log device detection (default = enable).
device-view-mode {regular | tree}	Set the devices/groups view mode (default = regular).
enc-algorithm {high | medium | low}	Set SSL communication encryption algorithms: • `high`: SSL communication using high encryption algorithms (default). • `medium`: SSL communication using high and medium encryption algorithms. • `low`: SSL communication using all available encryption algorithms.
fgfm-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}	Set the lowest SSL protocols for fgfmsd (default = tlsv1.2).
ha-member-auto-grouping {enable | disable}	Enable/disable automatically grouping HA members when the group name is unique in your network (default = enable).
hitcount_concurrent <integer>	Set the number of FortiGates that FortiAnalyzer polls at one time (10 - 500, default = 100).
hitcount_interval <integer>	Set the interval for getting the hit count from connected FortiGate devices, in seconds (60 - 86400, default = 300).
hostname <string>	FortiAnalyzer host name.
language {english | japanese | simch | spanish | trach}	GUI language: • `english`: English (default) • `japanese`: Japanese • `simch`: Simplified Chinese • `spanish`: Spanish • `trach`: Traditional Chinese
ldap-cache-timeout <integer>	LDAP cache timeout, in seconds (default =86400).
ldapconntimeout <integer>	LDAP connection timeout, in milliseconds (default = 60000).
lock-preempt {enable | disable}	Enable/disable the ADOM lock override (default = disable).
log-checksum {md5 | md5-auth | none}	Record log file hash value, timestamp, and authentication code at transmission or rolling: • `md5`: Record log file's MD5 hash value only. • `md5-auth`: Record log file's MD5 hash value and authentication code. • `none`: Do not record the log file checksum (default).
log-mode {analyzer | collector}	Set the log system operation mode (default = analyzer).
max-aggregation-tasks <integer>	Set the maximum number of concurrent tasks of a log aggregation session (1 - 10, default = 0).
max-log-forward <integer>	Set the maximum log forwarding and aggregation number (5 - 20).

Variable	Description
max-running-reports <integer>	Maximum running reports number (1 - 10, default = 1).
oftp-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}	Set the lowest SSL protocols for oftpd (default = tlsv1.2).
policy-hit-count {enable | disable}	Enable/disable show policy hit count (default= disable). The policy hit count is the number of sessions that match to a firewall policy on a FortiGate. When `policy-hit-count` is enabled, it collects all hits from all managed FortiGate devices. FortiAnalyzer sums up all hit counts for each policy package from the assigned FortiGate devices, and displays the hit count for each of the firewall rules.
policy-object-in-dual-pane {enable | disable}	Enable/disable show policies and objects in dual pane (default= disable).
pre-login-banner {enable | disable}	Enable/disable pre-login banner (default= disable).
pre-login-banner-message <string>	Set the pre-login banner message.
remoteauthtimeout <integer>	Remote authentication (RADIUS/LDAP) timeout, in seconds (default = 10).
search-all-adoms {enable | disable}	Enable/disable search all ADOMs for where-used queries (default= disable).
ssl-low-encryption {enable | disable}	Enable/disable SSL low-grade (40-bit) encryption (default= disable).
ssl-protocol {tlsv1.2 | tlsv1.1 | tlsv1.0 | sslv3}	Set the SSL protocols (default = tlsv1.2).
ssl-static-key-ciphers {enable | disable}	Enable/disable SSL static key ciphers (default = enable).
task-list-size <integer>	Set the maximum number of completed tasks to keep (default = 2000).
tftp	
timezone <integer>	The time zone for the FortiManager unit (default = Pacific Time). See Time zones on page 66.
tunnel-mtu <integer>	Set the maximum transportation unit (68 - 9000, default = 1500).
usg {enable | disable}	Enable/disable contacting only FortiGuard servers in the USA (default = enable).
webservice-proto {tlsv1.2 | tlsv1.1 | tlsv1.0 | sslv3 | sslv2}	Web Service connection (default = tlsv1.2).
workflow-max-sessions <integer>	Maximum number of workflow sessions per ADOM (100 - 1000, default = 500).

Example

The following command turns on daylight saving time, sets the FortiAnalyzer unit name to FMG3k, and chooses the Eastern time zone for US & Canada.

```
config system global
   set daylightsavetime enable
   set hostname FMG3k
   set timezone 12
end
```

Time zones

Integer	Time zone	Integer	Time zone
00	(GMT-12:00) Eniwetak, Kwajalein	40	(GMT+3:00) Nairobi
01	(GMT-11:00) Midway Island, Samoa	41	(GMT+3:30) Tehran
02	(GMT-10:00) Hawaii	42	(GMT+4:00) Abu Dhabi, Muscat
03	(GMT-9:00) Alaska	43	(GMT+4:00) Baku
04	(GMT-8:00) Pacific Time (US & Canada)	44	(GMT+4:30) Kabul
05	(GMT-7:00) Arizona	45	(GMT+5:00) Ekaterinburg
06	(GMT-7:00) Mountain Time (US & Canada)	46	(GMT+5:00) Islamabad, Karachi,Tashkent
07	(GMT-6:00) Central America	47	(GMT+5:30) Calcutta, Chennai, Mumbai, New Delhi
08	(GMT-6:00) Central Time (US & Canada)	48	(GMT+5:45) Kathmandu
09	(GMT-6:00) Mexico City	49	(GMT+6:00) Almaty, Novosibirsk
10	(GMT-6:00) Saskatchewan	50	(GMT+6:00) Astana, Dhaka
11	(GMT-5:00) Bogota, Lima, Quito	51	(GMT+6:00) Sri Jayawardenapura
12	(GMT-5:00) Eastern Time (US & Canada)	52	(GMT+6:30) Rangoon
13	(GMT-5:00) Indiana (East)	53	(GMT+7:00) Bangkok, Hanoi, Jakarta
14	(GMT-4:00) Atlantic Time (Canada)	54	(GMT+7:00) Krasnoyarsk
15	(GMT-4:00) La Paz	55	(GMT+8:00) Beijing,ChongQing, HongKong,Urumqi
16	(GMT-4:00) Santiago	56	(GMT+8:00) Irkutsk, Ulaanbaatar
17	(GMT-3:30) Newfoundland	57	(GMT+8:00) Kuala Lumpur, Singapore
18	(GMT-3:00) Brasilia	58	(GMT+8:00) Perth
19	(GMT-3:00) Buenos Aires, Georgetown	59	(GMT+8:00) Taipei
20	(GMT-3:00) Nuuk (Greenland)	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul
21	(GMT-2:00) Mid-Atlantic	61	(GMT+9:00) Yakutsk
22	(GMT-1:00) Azores	62	(GMT+9:30) Adelaide
23	(GMT-1:00) Cape Verde Is	63	(GMT+9:30) Darwin

Integer	Time zone	Integer	Time zone
24	(GMT) Casablanca, Monrovia	64	(GMT+10:00) Brisbane
25	(GMT) Greenwich Mean Time:Dublin, Edinburgh, Lisbon, London	65	(GMT+10:00) Canberra, Melbourne, Sydney
26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	66	(GMT+10:00) Guam, Port Moresby
27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	67	(GMT+10:00) Hobart
28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris	68	(GMT+10:00) Vladivostok
29	(GMT+1:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb	69	(GMT+11:00) Magadan
30	(GMT+1:00) West Central Africa	70	(GMT+11:00) Solomon Is., New Caledonia
31	(GMT+2:00) Athens, Istanbul, Minsk	71	(GMT+12:00) Auckland, Wellington
32	(GMT+2:00) Bucharest	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is
33	(GMT+2:00) Cairo	73	(GMT+13:00) Nuku'alofa
34	(GMT+2:00) Harare, Pretoria	74	(GMT-4:30) Caracas
35	(GMT+2:00) Helsinki, Riga,Tallinn	75	(GMT+1:00) Namibia
36	(GMT+2:00) Jerusalem	76	(GMT-5:00) Brazil-Acre)
37	(GMT+3:00) Baghdad	77	(GMT-4:00) Brazil-West
38	(GMT+3:00) Kuwait, Riyadh	78	(GMT-3:00) Brazil-East
39	(GMT+3:00) Moscow, St.Petersburg, Volgograd	79	(GMT-2:00) Brazil-DeNoronha

ha

Use this command to enable and configure FortiAnalyzer high availability (HA).

FortiAnalyzer HA clusters provide real-time redundancy in case a unit fails. Logs, data, and relevant system settings are securely synchronized across multiple FortiAnalyzer devices, and processing tasks can be shared to alleviate the load on the primary unit.

A FortiAnalyzer HA cluster can have a maximum of five units, all of which are visible on the network. All of the units must be from the same product series and in the same operating mode (analyzer or collector). HA is not supported when FortiManager features are enabled.

For more information, see the FortiAnalyzer Administration Guide.

Syntax

```
config system ha
   set group-id <integer>
   set group-name <name>
   set hb-interface
   set hb-interval <integer>
   set healthcheck {DB | fault-test}
   set initial-sync {true | false}
   set initial-sync-threads <integer>
   set load-balance (disable | round-robin}
   set log-sync {enable | disable}
   set mode {a-p | standalone}
   set password <passwd>
   set preferred-role
   set priority <integer>
   set private-clusterid
   set private-file-quota
   set private-hb-interval
   set private-hb-lost-threshold
   set private-mode
   set private-password
   set vip <ip_address>
   set vip-interface <port>
   config peer
      edit <peer_id_int>
         set ip <peer_ip_address>
         set serial-number <string>
         set status {enable | disable}
   end
end
```

Variable	Description
group-id <integer>	Set the HA group ID (1 - 255, default = 0).
group-name <name>	Set the HA group name.
hb-interface	
hb-interval <integer>	The time, in seconds, that a cluster unit waits between sending heartbeat packets. The heartbeat interval is also the amount of time that a cluster unit waits before expecting to receive a heartbeat packet from the other cluster unit (1 - 20, default = 1).
healthcheck {DB | fault-test}	Set the healthcheck options: • `DB` - Check that the database is running. • `fault-test` - Temp fault test.
initial-sync {true | false}	Synchronize data from the primary device before joining the HA cluster (default = true).
initial-sync-threads <integer>	Number of threads used for initial synchronization (1 - 15, default = 4).
load-balance (disable | round-robin}	Configure load balancing to secondary units (default = round-robin).

Variable	Description
log-sync {enable | disable}	Synchronize logs to backup FortiAnalyzer devices (default = enable).
mode {a-p | standalone}	Set the HA operating mode: Active-passive mode (`a-p`) or Standalone mode (`standalone`) (default = standalone).
password <passwd>	Set the HA group password.
priority <integer>	Set the runtime priority (80 - 120, default = 100).
preferrred-role {master | slave}	The preferred role of this unit (default = slave). The runtime role may be different.
private-clusterid	
private-file-quota	
private-hb-interval	
private-hb-lost-threshold	
private-mode	
private-password	
vip <ip_address>	Set the virtual IP address for the HA cluster.
vip-interface <port>	Set the virtual interface for configuring the virtual IP address.
Variables for `config peer` **subcommand**:	
<peer_id_int>	Add a peer and add the peer's IPv4 or IPv6 address and serial number.
ip <peer_ip_address>	Enter the IPv4 address of the peer FortiAnalyzer unit.
serial-number <string>	Enter the serial number of the peer FortiAnalyzer unit.
status {enable | disable}	Enter the status of the peer FortiAnalyzer unit (default = enable).

interface

Use this command to edit the configuration of a FortiAnalyzer network interface.

Syntax

```
config system interface
   edit <port_string>
      set status {up | down}
      set ip <ipv4address_mask>
      set allowaccess {fgfm http https https-logging ping snmp ssh telnet webservice}
      set speed {1000full | 100full | 100half | 10full | 10half | auto}
      set description <string>
      set alias <string>
      set mtu <integer>
      config ipv6
         set ip6-address <IPv6address prefix>
```

```
        set ip6-allowaccess {fgfm http https https-logging ping snmp ssh telnet webservice}
        set ip6-autoconf {enable | disable}
    end
end
```

Variable	Description
<port>	The port can be set to a port number such as port1, port2, port3, or port4. Different FortiAnalyzer models have different numbers of ports.
status {up | down}	Start (up) or stop (down) the interface (default = up). If the interface is stopped it does not accept or send packets. If you stop a physical interface, VLAN interfaces associated with it also stop.
ip <ipv4_mask>	Enter the interface IPv4 address and netmask. The IPv4 address cannot be on the same subnet as any other interface.
allowaccess {fgfm http https https-logging ping snmp ssh telnet webservice}	Enter the types of management access permitted on this interface. Separate multiple selected types with spaces. If you want to add or remove an option from the list, retype the list as required.
speed {1000full 100full 100half 10full 10half auto}	Enter the speed and duplexing the network port uses: • `100full`: 100M full-duplex • `100half`: 100M half-duplex • `10full`: 10M full-duplex • `10half`: 10M half-duplex • `auto`: Automatically negotiate the fastest common speed (default)
description <string>	Enter a description of the interface (character limit = 63).
alias <string>	Enter an alias for the interface.
mtu <integer>	Set the maximum transportation unit (68 - 9000, default = 1500).
Variables for `ipv6` subcommand:	
ip6-address <ipv6 prefix>	IPv6 address/prefix of interface.
ip6-allowaccess {fgfm http https https-logging ping snmp ssh telnet webservice}	Allow management access to the interface.
ip6-autoconf {enable | disable}	Enable/disable address automatic configuration (SLAAC) (default = enable).

Example

This example shows how to set the FortiAnalyzer port1 interface IPv4 address and network mask to `192.168.100.159 255.255.255.0`, and the management access to `ping`, `https`, and `ssh`.

```
config system interface
    edit port1
        set allowaccess ping https ssh
        set ip 192.168.110.26 255.255.255.0
        set status up
    end
```

locallog

Use the following commands to configure local log settings.

locallog setting

Use this command to configure locallog logging settings.

Syntax

```
config system locallog setting
   set log-interval-dev-no-logging <integer>
   set log-interval-disk-full <integer>
   set log-interval-gbday-exceeded <integer>
end
```

Variable	Description
log-interval-dev-no-logging <integer>	Interval for logging the event of no logs received from a device, in minutes (default = 1400).
log-interval-disk-full <integer>	Interval for logging the event of disk full, in minutes (default = 5).
log-interval-gbday-exceeded <integer>	Interval for logging the event of the GB/Day license exceeded, in minutes (default = 1400).

locallog disk setting

Use this command to configure the disk settings for uploading log files, including configuring the severity of log levels.

- `status` must be enabled to view `diskfull`, `max-log-file-size` and `upload` variables.
- `upload` must be enabled to view/set other `upload*` variables.

Syntax

```
config system locallog disk setting
   set status {enable | disable}
   set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
   set max-log-file-size <integer>
   set roll-schedule {none | daily | weekly}
   set roll-day <string>
   set roll-time <hh:mm>
   set diskfull {nolog | overwrite}
   set log-disk-full-percentage <integer>
   set upload {enable | disable}
   set uploadip <ipv4_address>
   set server-type {FAZ | FTP | SCP | SFTP}
   set uploadport <integer>
   set uploaduser <string>
```

```
    set uploadpass <passwd>
    set uploaddir <string>
    set uploadtype <event>
    set uploadzip {enable | disable}
    set uploadsched {enable | disable}
    set upload-time <hh:mm>
    set upload-delete-files {enable | disable}
end
```

Variable	Description
status {enable | disable}	Enable/disable logging to the local disk (default = enable)
severity {emergency | alert | critical | error | warning | notification | information | debug }	Select the logging severity level. The FortiAnalyzer unit logs all messages at and above the logging severity level you select. • `emergency`: The unit is unusable. • `alert`: Immediate action is required. • `critical`: Functionality is affected. • `error`: Functionality is probably affected. • `warning`: Functionality might be affected. • `notification`: Information about normal events. • `information`: General information about unit operations (default). • `debug`: Information used for diagnosis or debugging.
max-log-file-size <integer>	Enter the size at which the log is rolled, in megabytes (1 - 1024, default = 100).
roll-schedule {none | daily | weekly}	Enter the period for the scheduled rolling of a log file: • `none`: Not scheduled; the log rolls when `max-log-file-size` is reached (default). • `daily`: Every day. • `weekly`: Every week.
roll-day {sunday | monday | tuesday | wednesday | thursday | friday | saturday}	Enter the day for the scheduled rolling of a log file (default = sunday).
roll-time <hh:mm>	Enter the time for the scheduled rolling of a log file.
diskfull {nolog | overwrite}	Enter action to take when the disk is full: • `nolog`: stop logging • `overwrite`: overwrites oldest log entries (default)
log-disk-full-percentage <integer>	Enter the percentage at which the log disk will be considered full (50 - 90, default = 80).
upload {enable | disable}	Enable/disable uploading of logs when rolling log files (default = disable).
uploadip <ipv4_address>	Enter IPv4 address of the destination server.
server-type {FTP | SCP | SFTP}	Enter the server type to use to store the logs: • `FTP`: upload via FTP (default) • `SCP`: upload via SCP • `SFTP`: upload via SFTP

Variable	Description
uploadport <integer>	Enter the port to use when communicating with the destination server (1 - 65535, default = 0).
uploaduser <string>	Enter the user account on the destination server.
uploadpass <passwd>	Enter the password of the user account on the destination server (character limit = 127).
uploaddir <string>	Enter the destination directory on the remote server.
uploadtype <event>	Enter to upload the event log files (default = event).
uploadzip {enable | disable}	Enable to compress uploaded log files (default = disable).
uploadsched {enable | disable}	Enable to schedule log uploads (default = disable).
upload-time <hh:mm>	Enter to configure when to schedule an upload.
upload-delete-files {enable | disable}	Enable/disable deleting log files after uploading (default = enable).

Example

In this example, the logs are uploaded to an upload server and are not deleted after they are uploaded.

```
config system locallog disk setting
   set status enable
   set severity information
   set max-log-file-size 1000MB
   set roll-schedule daily
   set upload enable
   set uploadip 10.10.10.1
   set uploadport port 443
   set uploaduser myname2
   set uploadpass 12345
   set uploadtype event
   set uploadzip enable
   set uploadsched enable
   set upload-time 06:45
   set upload-delete-file disable
end
```

locallog filter

Use this command to configure filters for local logs. All keywords are visible only when `event` is `enabled`.

Syntax

```
config system locallog [memory | disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 |
      syslogd | syslogd2 | syslogd3] filter
   set devcfg {enable | disable}
   set devops {enable | disable}
   set diskquota {enable | disable}
```

```
    set dm {enable | disable}
    set dvm {enable | disable}
    set ediscovery {enable | disable}
    set epmgr {enable | disable}
    set event {enable | disable}
    set eventmgmt {enable | disable}
    set faz {enable | disable}
    set fazha {enable | disable}
    set fazsys {enable | disable}
    set fgd {enable | disable}
    set fgfm {enable | disable}
    set fips {enable | disable}
    set fmgws {enable | disable}
    set fmlmgr {enable | disable}
    set fmwmgr {enable | disable}
    set fortiview {enable | disable}
    set glbcfg {enable | disable}
    set ha {enable | disable}
    set hcache {enable | disable}
    set iolog {enable | disable}
    set logd {enable | disable}
    set logdb {enable | disable}
    set logdev {enable | disable}
    set logfile {enable | disable}
    set logging {enable | disable}
    set lrmgr {enable | disable}
    set objcfg {enable | disable}
    set report {enable | disable}
    set rev {enable | disable}
    set rtmon {enable | disable}
    set scfw {enable | disable}
    set scply {enable | disable}
    set scrmgr {enable | disable}
    set scvpn {enable | disable}
    set system {enable | disable}
    set webport {enable | disable}
end
```

Variable	Description
devcfg {enable | disable}	Enable/disable logging device configuration messages (default = enable).
devops {enable | disable}	Enable/disable managed device's operations messages (default = enable).
diskquota {enable | disable}	Enable/disable logging FortiAnalyzer disk quota messages (default = enable).
dm {enable | disable}	Enable/disable logging deployment manager messages (default = enable).
dvm {enable | disable}	Enable/disable logging device manager messages (default = enable).
ediscovery {enable | disable}	Enable/disable logging device manager messages (default = enable).
epmgr {enable | disable}	Enable/disable logging endpoint manager messages (default = enable).
event {enable | disable}	Enable/disable configuring log filter messages (default = enable).
eventmgmt {enable | disable}	Enable/disable logging FortiAnalyzer event handler messages (default = enable).

Variable	Description
faz {enable | disable}	Enable/disable logging FortiAnalyzer messages (default = enable).
fazha {enable | disable}	Enable/disable logging FortiAnalyzer messages (default = enable).
fazsys {enable | disable}	Enable/disable logging FortiAnalyzer HA system messages (default = enable).
fgd {enable | disable}	Enable/disable logging FortiGuard service messages (default = enable).
fgfm {enable | disable}	Enable/disable logging FortiGate/FortiManager communication protocol messages (default = enable).
fips {enable | disable}	Enable/disable logging FIPS messages (default = enable).
fmgws {enable | disable}	Enable/disable logging web service messages (default = enable).
fmlmgr {enable | disable}	Enable/disable logging FortiMail manager messages (default = enable).
fmwmgr {enable | disable}	Enable/disable logging firmware manager messages (default = enable).
fortiview {enable | disable}	Enable/disable logging FortiAnalyzer FortiView messages (default = enable).
glbcfg {enable | disable}	Enable/disable logging global database messages (default = enable).
ha {enable | disable}	Enable/disable logging high availability activity messages (default = enable).
hcache {enable | disable}	Enable/disable logging hcache messages (default = enable).
iolog {enable | disable}	Enable/disable input/output log activity messages (default = enable).
logd {enable | disable}	Enable/disable logd messages (default = enable).
logdb {enable | disable}	Enable/disable logging FortiAnalyzer log DB messages (default = enable).
logdev {enable | disable}	Enable/disable logging FortiAnalyzer log device messages (default = enable).
logfile {enable | disable}	Enable/disable logging FortiAnalyzer log file messages (default = enable).
logging {enable | disable}	Enable/disable logging FortiAnalyzer logging messages (default = enable).
lrmgr {enable | disable}	Enable/disable logging log and report manager messages (default = enable).
objcfg {enable | disable}	Enable/disable logging object configuration (default = enable).
report {enable | disable}	Enable/disable logging FortiAnalyzer report messages (default = enable).
rev {enable | disable}	Enable/disable logging revision history messages (default = enable).
rtmon {enable | disable}	Enable/disable logging real-time monitor messages (default = enable).
scfw {enable | disable}	Enable/disable logging firewall objects messages (default = enable).
scply {enable | disable}	Enable/disable logging policy console messages (default = enable).
scrmgr {enable | disable}	Enable/disable logging script manager messages (default = enable).
scvpn {enable | disable}	Enable/disable logging VPN console messages (default = enable).
system {enable | disable}	Enable/disable logging system manager messages (default = enable).
webport {enable | disable}	Enable/disable logging web portal messages (default = enable).

Example

In this example, the local log filters are log and report manager, and system settings. Events in these areas of the FortiAnalyzer unit will be logged.

```
config system locallog filter
   set event enable
   set lrmgr enable
   set system enable
end
```

locallog fortianalyzer (fortianalyzer2, fortianalyzer3) setting

Use this command to enable or disable, and select the severity threshold of, remote logging to the FortiAnalyzer units. You can configure up to three FortiAnalyzer devices.

The severity threshold required to forward a log message to the FortiAnalyzer unit is separate from event, syslog, and local logging severity thresholds.

Syntax

```
config system locallog [fortianalyzer | fortianalyzer2 | fortianalyzer3] setting
   set reliable {enable | disable}
   set secure-connection {enable | disable}
   set server-ip <ipv4_address>
   set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
   set status {disable | realtime | upload}
   set upload-time <hh:mm>
end
```

Variable	Description
reliable {enable | disable}	Enable/disable reliable realtime logging (default = disable).
secure-connection {enable | disable}	Enable/disable connection secured by TLS/SSL (default = disable). This variable is available when `status` is `realtime` or `upload`.
server-ip <ipv4_address>	Remote FortiAnalyzer server IP address. Enter an IPv4 address in the format xxx.xxx.xxx.xxx.
severity {emergency | alert | critical | error | warning | notification | information | debug }	Select the logging severity level (default = notification). The FortiAnalyzer unit logs all messages at and above the logging severity level you select.
status {disable | realtime | upload}	Set the log to FortiAnalyzer status: • `disable`: Do not log to FortiAnalyzer (default). • `realtime`: Log to FortiAnalyzer in realtime. • `upload`: Log to FortiAnalyzer at a scheduled time.
upload-time <hh:mm>	Set the time to upload local log files (default = 00:00).

Example

You might enable remote logging to the FortiAnalyzer unit configured. Events at the information level and higher, which is everything except debug level events, would be sent to the FortiAnalyzer unit.

```
config system locallog fortianalyzer setting
   set status enable
   set severity information
end
```

locallog memory setting

Use this command to configure memory settings for local logging purposes.

Syntax

```
config system locallog memory setting
   set diskfull {nolog | overwrite}
   set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
   set status <enable | disable>
end
```

Variable	Description
diskfull {nolog | overwrite}	Enter the action to take when the disk is full: • `nolog`: Stop logging when disk full • `overwrite`: Overwrites oldest log entries
severity {emergency | alert | critical | error | warning | notification | information | debug}	Select the logging severity level (default = notification). The FortiAnalyzer unit logs all messages at and above the logging severity level you select.
status <enable | disable>	Enable/disable logging to the memory buffer (default = disable).

Example

This example shows how to enable logging to memory for all events at the notification level and above. At this level of logging, only information and debug events will not be logged.

```
config system locallog memory
   set severity notification
   set status enable
end
```

locallog syslogd (syslogd2, syslogd3) setting

Use this command to configure the settings for logging to a syslog server. You can configure up to three syslog servers: syslogd, syslogd2 and syslogd3.

Syntax

```
config system locallog {syslogd | syslogd2 | syslogd3} setting
   set csv {enable | disable}
   set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel |
        local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail |
        news | ntp | syslog | user | uucp}
   set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
   set status {enable | disable}
   set syslog-name <string>
end
```

Variable	Description
csv {enable | disable}	Enable/disable producing the log in comma separated value (CSV) format (default = disable). If you do not enable CSV format the FortiAnalyzer unit produces space separated log files.
facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp | syslog | user | uucp}	Enter the facility type (default = local7). The facility identifies the source of the log message to syslog. Change `facility` to distinguish log messages from different FortiAnalyzer units so you can determine the source of the log messages. `local0` to `local7` are reserved for local use.
severity {emergency | alert | critical | error | warning | notification | information | debug}	Select the logging severity level (default = notification). The FortiAnalyzer unit logs all messages at and above the logging severity level you select.
status {enable | disable}	Enable/disable logging to the remote syslog server (default = disable).
syslog-name <string>	Enter the remote syslog server name.

Use the show command to display the current configuration if it has been changed from its default value:

```
show system locallog syslogd setting
```

Example

In this example, the logs are uploaded to a syslog server at IPv4 address `10.10.10.8`. The FortiAnalyzer unit is identified as facility `local0`.

```
config system locallog syslogd setting
   set facility local0
   set server 10.10.10.8
   set status enable
   set severity information
end
```

log

Use the following commands to configure log settings.

log alert

Use this command to configure log based alert settings.

Syntax

```
config system log alert
   set max-alert-count <integer>
end
```

Variable	Description
max-alert-count <integer>	Maximum number of alerts supported (100 - 50000, default = 10000).

log ioc

Use this command to configure log based IoC (Indicators of Compromise) settings.

Syntax

```
config system log ioc
   set notification {enable | disable}
   set notification-throttle <integer>
   set status
end
```

Variable	Description
notification {enable | disable}	Enable/disable IoC notification (default = enable).
notification-throttle <integer>	Set the minute value for throttling the rate of IoC notifications (1 - 10080, default = 1440).
status	Enable/disable the IoC feature (default = enable).

log mail-domain

Use this command to configure FortiMail domain settings.

Syntax

```
config system log mail-domain
```

```
    edit <id>
       set devices <string>
       set domain <string>
       set vdom <string>
end
```

Variable	Description
<id>	The ID of the FortiMail domain.
devices <string>	The device IDs for domain to VDOM mapping, separated by commas (default = All_FortiMails). For example: `FEVM020000000000,FEVM020000000001`
domain <string>	The FortiMail domain.
vdom <string>	The VDOM name that is mapping to the FortiMail domain.

log settings

Use this command to configure settings for logs.

Syntax

```
config system log settings
   set browse-max-logfiles <integer>
   set dns-resolve-dstip {enable | disable}
   set download-max-logs <integer>
   set FAC-custom-field1 <string>
   set FAZ-custom-field1 <string>
   set FCH-custom-field1 <string>
   set FCT-custom-field1 <string>
   set FDD-custom-field1 <string>
   set FGT-custom-field1 <string>
   set FMG-custom-field1 <string>
   set FML-custom-field1 <string>
   set FPX-custom-field1 <string>
   set FSA-custom-field1 <string>
   set FWB-custom-field1 <string>
   set ha-auto-migrate {enable | disable}
   set import-max-logfiles <integer>
   set log-file-archive-name {basic | extended}
   set sync-search-timeout <integer>
   config rolling-regular
      set days {fri | mon| sat | sun | thu | tue | wed}
      set del-files {enable | disable}
      set directory <string>
      set file-size <integer>
      set gzip-format {enable | disable}
      set hour <integer>
      set ip <ipv4_address>
      set ip2 <ipv4_address>
      set ip3 <ipv4_address>
      set log-format {csv | native | text}
```

```
        set min <integer>
        set password <passwd>
        set password2 <passwd>
        set password3 <passwd>
        set server-type {ftp | scp | sftp}
        set upload {enable | disable}
        set upload-hour <integer>
        set upload-mode {backup | mirror}
        set upload-trigger {on-roll | on-schedule}
        set username <string>
        set username2 <string>
        set username3 <string>
        set when {daily | none | weekly}
    end
end
```

Variable	Description
browse-max-logfiles <integer>	Maximum number of log files for each log browse attempt, per ADOM (default = 10000).
dns-resolve-stip {enable | disable}	Enable/disable resolving destination IP by DNS (default = disable).
download-max-logs <integer>	Maximum number of logs for each log download attempt (default = 500000).
FAC-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FAZ-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FCH-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FCT-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FDD-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FGT-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FMG-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FML-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FPX-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FSA-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
FWB-custom-field1 <string>	Enter a name of the custom log field to index (character limit = 31).
ha-auto-migrate {enable | disable}	Enabled/disable automatically merging HA member's logs to HA cluster (default = disable).
import-max-logfiles <integer>	Maximum number of log files for each log import attempt (default = 10000).
log-file-archive-name {basic | extended}	Log file name format for archiving. • `basic`: Basic format for log archive file name (default), for example: `FGT20C0000000001.tlog.1417797247.log`. • `extended`: Extended format for log archive file name, for example: `FGT20C0000000001.2014-12-05-08:34:58.tlog.1417797247.log`.

Variable	Description
sync-search-timeout <integer>	The maximum amount of time that a log search session can run in synchronous mode, in seconds (1 - 86400, default = 60).
Variables for `config rolling-regular` **subcommand**:	
days {fri | mon| sat | sun | thu | tue | wed}	Log files rolling schedule (days of the week). When `when` is set to `weekly`, you can configure `days`, `hour`, and `min` values.
del-files {enable | disable}	Enable/disable log file deletion after uploading (default = disable).
directory <string>	The upload server directory (character limit = 127).
file-size <integer>	Roll log files when they reach this size, in megabytes (10 - 1000, default = 200).
gzip-format {enable | disable}	Enable/disable compression of uploaded log files (default = disable).
hour <integer>	The hour of the day that log files are rolled (0 - 23, default = 0).
ip <ipv4_address> ip2 <ipv4_address> ip3 <ipv4_address>	Upload server IPv4 addresses. Configure up to three servers.
log-format {csv | native | text}	Format of uploaded log files: • `csv`: CSV (comma-separated value) format. • `native`: Native format (text or compact) (default). • `text`: Text format (convert if necessary).
min <integer>	The minute of the hour that log files are rolled (0 - 59, default = 0).
password <passwd> password2 <passwd> password3 <passwd>	Upload server log in passwords (character limit = 128).
server-type {ftp | scp | sftp}	Upload server type (default = ftp).
upload {enable | disable}	Enable/disable log file uploads (default = disable).
upload-hour <integer>	The hour of the day that log files are uploaded (0 - 23, default = 0).
upload-mode {backup | mirror}	Configure upload mode with multiple servers. Servers are tried then used one after the other upon failure to connect. • `backup`: Servers are attempted and used one after the other upon failure to connect (default). • `mirror`: All configured servers are attempted and used.
upload-trigger {on-roll | on-schedule}	Event triggering log files upload: • `on-roll`: Upload log files after they are rolled (default). • `on-schedule`: Upload log files daily.
username <string> username2 <string> username3 <string>	Upload server log in usernames (character limit = 35).
when {daily | none | weekly}	Roll log files periodically:

Variable	Description
	• `daily`: Roll log files daily. • `none`: Do not roll log files periodically (default). • `weekly`: Roll log files on certain days of week.

log-fetch

Use the following commands to configure log fetching.

log-fetch client-profile

Use this command to configure the fetching client settings.

Syntax

```
config system log-fetch client-profile
   edit <id>
      set client-adom <string>
      set data-range {custom}
      set data-range-value <integer>
      set end-time <hh:mm> <yyyy/mm/dd>
      set index-fetch-logs {enable | disable}
      set log-filter-status {enable | disable}
      set log-filter-logic {and | or}
      set name <string>
      set password <passwd>
      set secure-connection {enable | disable}
      set server-adom <string>
      set server-ip <ip>
      set start-time <hh:mm> <yyyy/mm/dd>
      set sync-adom-config {enable | disable}
      set user <string>
      config device-filter
         edit <id>
            set adom <string>
            set device <device>
            set vdom <string>
         next
      config log-filter
         edit <id>
            set field <string>
            set oper {= | != | < | > | <= | >= | contain | not-contain | match}
            set value <string>
         next
      next
   end
end
```

Variable	Description
<id>	The log-fetch client profile ID.
client-adom <string>	Log-fetch client side's adom name.
data-range {custom}	The data range settings for the fetched logs, which is always custom.
data-range-value <integer>	An integer representing the data range value.
end-time <hh:mm> <yyyy/mm/dd>	Set the end date and time of the data-range.
index-fetch-logs {enable | disable}	Enable/disable indexing logs automatically after fetching logs (default = enabled).
log-filter-status {enable | disable}	Enable/Disable log-filter (default = disabled).
log-filter-logic {and | or}	Set the logic for the log filters (default = or).
name <string>	The name of log-fetch client profile.
password <passwd>	The log-fetch server password.
secure-connection {enable | disable}	Enable/disable protecting log-fetch connection with TLS/SSL (default = enabled).
server-adom <string>	Log-fetch server side's adom name.
server-ip <ip>	The log fetch server IPv4 address.
start-time <hh:mm> <yyyy/mm/dd>	Set the start date and time of the data-range. The start date should be earlier than the end date.
sync-adom-config {enable | disable}	Enable/disable ADOM configuration synchronization.
user <string>	The log-fetch server username.
Variables for `config device-filter` **subcommand**:	
<id>	Add or edit a device filter.
adom <string>	Enter the ADOM name.
device <device>	Enter the device name or serial number.
vdom <string>	Enter the VDOM, if required.
Variables for `config log-filter` **subcommand**:	
<id>	The log filter ID.
field <string>	Enter the field name.
oper {= | != | < | > | <= | >= | contain | not-contain | match}	Set the filter operator.
value <string>	Enter the field filter operand or free-text matching expression.

log-fetch server-setting

Use this command to configure the fetching server settings.

Syntax

```
config system log-fetch server-setting
   set max-conn-per-session <integer>
   set max-sessions <integer>
   set user <string>
end
```

Variable	Description
max-conn-per-session <integer>	The maximum number of concurrent file download connections per session (default = 3).
max-sessions <integer>	The maximum number of concurrent fetch sessions (default = 1).
session-timeout <integer>	Set the fetch session timeout period, in minutes (default = 10). This option is only available in server mode.

log-forward

Use the following commands to configure log forwarding.

Syntax

```
config system log-forward
   edit <id>
      set mode {aggregation | disable | forwarding}
      set agg-archive-types {Web_Archive Secure_Web_Archive Email_Archive File_Transfer_
          Archive IM_Archive MMS_Archive AV_Quarantine IPS_Packets}
      set agg-logtypes {none app-ctrl attack content dlp emailfilter event generic history
          traffic virus webfilter netscan fct-event fct-traffic fct-netscan waf gtp dns
          ssh}
      set agg-password <passwd>
      set agg-time <integer>
      set agg-user <string>
      set fwd-archives {enable | disable}
      set fwd-archive-types {Web_Archive Email_Archive IM_Archive File_Transfer_Archive MMS_
          Archive AV_Quarantine IPS_Packets EDISC_Archive}
      set fwd-facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp |
          kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 |
          lpr | mail | news | ntp | syslog | user | uucp}
      set fwd-log-source-ip {local_ip | original_ip}
      set fwd-max-delay {1min | 5min | realtime}
      set fwd-reliable {enable | disable}
      set fwd-secure {enable | disable}
      set fwd-server-type {cef | fortianalyzer | syslog}
      set log-field-exclusion-status {enable | disable}
```

```
        set log-filter-logic {and | or}
        set log-filter-status {enable | disable}
        set proxy-service {enable | disable}
        set proxy-service-priority <integer>
        set server-device <string>
        set server-ip <ipv4_address>
        set server-name <string>
        set server-port <integer>
        set signature <integer>
        set sync-metadata [sf-topology | interface-role | device | endusr-avatar]
        config device-filter
           edit <id>
              set action {include | exclude}
              set device <string>
           end
        config log-field-exclusion
           edit <id>
              set dev-type {FortiGate | FortiMail | FortiManager | FortiAnalyzer | FortiWeb |
                   FortiCache | FortiSandbox | FortiDDoS | Syslog}
              set field-list <string>
              set log-type {app-ctrl | attack | content | dlp | emailfilter | event | generic |
                   history | traffic | virus | voip | webfilter | netscan | waf | gtp | dns |
                   ssh | ANY-TYPE}
           end
        config log-filter
           edit <id>
              set field {type | logid | level | devid | vd | srcip | srcintf | srcport | dstip
                   | dstintf | dstport | user | group | free-text }
              set oper {= | != | < | > | <= | >= | contain | not-contain | match}
              set value {traffic | event | utm}
           end
     end
```

Variable	Description
<id>	Enter the log aggregation ID that you want to edit.
mode {aggregation | disable | forwarding}	Log aggregation mode: • `aggregation`: Aggregate logs to FortiAnalyzer • `disable`: Do not forward or aggregate logs (default) • `forwarding`: Forward logs to the FortiAnalyzer
agg-archive-types {Web_Archive Secure_Web_Archive Email_ Archive File_Transfer_Archive IM_Archive MMS_Archive AV_ Quarantine IPS_Packets}	Archive type (default = all options). This command is only available when the mode is set to `aggregation`.
agg-logtypes {none app-ctrl attack content dlp emailfilter event generic history traffic virus webfilter netscan fct-event fct-traffic fct-netscan waf gtp dns ssh}	Log type (default = all options). This command is only available when the mode is set to `aggregation`.

Variable	Description
agg-password <passwd>	Log aggregation access password for server. This command is only available when the mode is set to `aggregation`.
agg-time <integer>	Daily at the selected time (0 - 23, default = 0). This command is only available when the mode is set to `aggregation`.
agg-user <string>	Log aggregation access user name for server. This command is only available when the mode is set to `aggregation`.
fwd-archives {enable | disable}	Enable/disable forwarding archives (default = enable). This command is only available when the mode is set to `forwarding`.
fwd-archive-types {Web_Archive Email_Archive IM_Archive File_ Transfer_Archive MMS_Archive AV_Quarantine IPS_Packets EDISC_Archive}	Set the forwarding archive types (default = all options). This command is only available when the mode is set to `forwarding`.
fwd-facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp | syslog | user | uucp}	Facility for remote syslog (default = local7). • `alert`: Log alert • `audit`: Log audit • `auth`: Security/authorization messages • `authpriv`: Security/authorization messages (private) • `clock`: Clock daemon • `cron`: Clock daemon • `daemon`: System daemons • `ftp`: FTP daemon • `kernel`: Kernel messages • `local0`, `local1`, `local2`, `local3`, `local4`, `local5`, `local6`, `local7`: Reserved for local use • `lpr`: Line printer subsystem • `mail`: Mail system • `news`: Network news subsystem • `ntp`: NTP daemon • `syslog`: Messages generated internally by `syslogd` • `user`: Random user level messages • `uucp`: Network news subsystem This command is only available when the mode is set to `forwarding`.
fwd-log-source-ip {local_ip | original_ip}	The logs source IP address (default = local_ip). This command is only available when the mode is set to `forwarding`.
fwd-max-delay {1min | 5min | realtime}	The maximum delay for near realtime log forwarding. • `1min`: Near realtime forwarding with up to one minute delay. • `5min`: Near realtime forwarding with up to five minutes delay (default). • `realtime`: Realtime forwarding, no delay. This command is only available when the mode is set to `forwarding`.

Variable	Description
fwd-reliable {enable | disable}	Enable/disable reliable logging (default = disable). This command is only available when the mode is set to `forwarding`. `fwd-remote-server` must be `syslog` to support reliable forwarding.
fwd-secure {enable | disable}	Enable/disable TLS/SSL secured reliable logging (default = disable). This command is only available when the mode is set to `forwarding`, `fwd-reliable` is enabled, and `fwd-server-type` is set to `syslog`.
fwd-server-type {cef | fortianalyzer | syslog}	Forwarding all logs to a CEF (Common Event Format) server, syslog server, or the FortiAnalyzer device (default = fortianalyzer). This command is only available when the mode is set to `forwarding`.
log-field-exclusion-status {enable | disable}	Enable/disable log field exclusion list (default = disable). This command is only available when the mode is set to `forwarding` and `fwd-server-type` is set to `cef` or `syslog`.
log-filter-logic {and | or}	Logic operator used to connect filters (default = or). This command is only available when `log-filter-status` is enabled.
log-filter-status {enable | disable}	Enable/disable log filtering (default = disable). This command is only available when the mode is set to `forwarding`.
proxy-service {enable | disable}	Enable/disable proxy service under collector mode (default = enable). This command is only available when the mode is set to `forwarding`.
proxy-service-priority <integer>	Proxy service priority from 1 (lowest) to 20 (highest) (default = 10). This command is only available when the mode is set to `forwarding`.
server-device <id>	Log aggregation server device ID.
server-ip <ipv4_address>	Remote server IPv4 address.
server-name <string>	Log aggregation server name.
server-port <integer>	Enter the server listen port (1 - 65535, default = 514). This command is only available when the mode is set to `forwarding`.
signature <integer>	This field is auto-generated and should not be set.
sync-metadata [sf-topology | interface-role | device | endusr-avatar]	Synchronizing metadata types: • `sf-topology`: Security Fabric topology • `interface-role`: Interface Role • `device`: Device information • `endusr-avatar`: End-user avatar This command is only available when the mode is set to `forwarding`.
Variables for `config device-filter` **subcommand**:	
<id>	Enter the device filter ID or enter a number to create a new entry.
action {include | exclude}	Include/exclude the specified device (default = include).
device <string>	Device ID of log client devices, or all of a device type.
Variables for `config log-field-exclusions` **subcommand**:	

Variable	Description
This command is only available when the `mode` is set to `forwarding` and `log-field-exclusions-status` is set to `enable`.	
<id>	Enter a device filter ID or enter a number to create a new entry.
dev-type {FortiGate | FortiMail | FortiManager | FortiAnalyzer | FortiWeb | FortiCache | FortiSandbox | FortiDDoS | Syslog}	The device type (default = FortiGate).
field-list <string>	The field type. Enter a comma separated list from the available fields.
log-type {app-ctrl | attack | content | dlp | emailfilter | event | generic | history | traffic | virus | voip | webfilter | netscan | waf | gtp | dns | ssh | ANY-TYPE}	The log type (default = traffic).
Variables for `config log-filter` **subcommand**: This command is only available when the `mode` is set to `forwarding` and `log-field-status` is set to `enable`.	
<id>	Enter the log filter ID or enter a number to create a new entry.
field {type | logid | level | devid | vd | srcip | srcintf | srcport | dstip | dstintf | dstport | user | group | free-text}	Field name (default = type).
oper {= | != | < | > | <= | >= | contain | not-contain | match}	Field filter operator (default = =).
value {traffic | event | utm}	Field filter operand or free-text matching expression.

log-forward-service

Use the following commands to configure log aggregation service.

This command is not available on all models.

Syntax

```
config system log-forward-service
   set accept-aggregation {enable | disable}
   set aggregation-disk-quota <integer>
end
```

Variable	Description
accept-aggregation {enable | disable}	Enable/disable accept log aggregation option (default = disable).
aggregation-disk-quota <integer>	Aggregated device disk quota on the server, in megabytes (default = 2000).

mail

Use this command to configure mail servers on your FortiAnalyzer unit.

Syntax

```
config system mail
   edit <id>
      set auth {enable | disable}
      set passwd <passwd>
      set port <integer>
      set secure-option {default | none | smtps | starttls}
      set server <string>
      set user <string>
   end
```

Variable	Description
<id>	Enter the mail service ID of the entry you would like to edit or type a new name to create an entry (character limit = 63).
auth {enable | disable}	Enable/disable authentication (default = disable).
passwd <passwd>	Enter the SMTP account password value (character limit = 63).
port <integer>	Enter the SMTP server port (1 - 65535, default = 25).
secure-option {default | none | smtps | starttls}	Select the communication secure option: • `default`:Try STARTTLS, proceed as plain text communication otherwise (default). • `none`: Communication will be in plain text format. • `smtps`: Communication will be protected by SMTPS. • `starttls`: Communication will be protected by STARTTLS.
server <string>	Enter the SMTP server name.
user <string>	Enter the SMTP account user name.

metadata

Use this command to add additional information fields to the administrator accounts of your FortiAnalyzer unit.

This command creates the metadata fields. Use `config system admin user` to add data to the metadata fields.

Syntax

```
config system metadata admins
   edit <fieldname>
      set fieldlength {20 | 255 | 50}
      set importance {optional | required}
      set status {enable | disable}
   end
```

Variable	Description
<fieldname>	Enter the name of the field.
fieldlength {20 | 255 | 50}	Select the maximum number of characters allowed in this field (default = 50).
importance {optional | required}	Select if this field is required or optional when entering standard information (default = required).
status {enable | disable}	Enable/disable the metadata (default = enabled).

ntp

Use this command to configure automatic time setting using a network time protocol (NTP) server.

Syntax

```
config system ntp
   set status {enable | disable}
   set sync_interval <string>
   config ntpserver
      edit <id>
         set ntpv3 {enable | disable}
         set authentication {enable | disable}
         set key <passwd>
         set key-id <integer>
         set server <string>
      end
end
```

Variable	Description
status {enable | disable}	Enable/disable NTP time setting (default = disable).

Variable	Description
sync_interval <string>	Enter how often the FortiManager unit synchronizes its time with the NTP server, in minutes (1 - 1440, default = 60).
Variables for `config ntpserver` **subcommand**:	
<id>	Time server ID.
ntpv3 {enable | disable}	Enable/disable NTPv3 (default = disable).
authentication {enable | disable}	Enable/disable MD5 authentication (default = disable).
key <passwd>	The authentication key (character limit = 63).
key-id <integer>	The key ID for authentication (default = 0).
server <string>	Enter the IPv4 address or fully qualified domain name of the NTP server.

password-policy

Use this command to configure access password policies.

Syntax

```
config system password-policy
   set status {enable | disable}
   set minimum-length <integer>
   set must-contain {lower-case-letter non-alphanumeric number upper-case-letter}
   set change-4-characters {enable | disable}
   set expire <integer>
end
```

Variable	Description
status {enable | disable}	Enable/disable the password policy (default = disable).
minimum-length <integer>	Set the password's minimum length (8 - 256, default = 8).
must-contain {lower-case-letter non-alphanumeric number upper-case-letter}	Characters that a password must contain. • `lower-case-letter`: the password must contain at least one lower case letter • `non-alphanumeric`: the password must contain at least one non-alphanumeric characters • `number`: the password must contain at least one number • `upper-case-letter`: the password must contain at least one upper case letter.
change-4-characters {enable | disable}	Enable/disable changing at least 4 characters for a new password (default = disable).
expire <integer>	Set the number of days after which admin users' passwords will expire (0 - 3650, 0 = never, default = 0).

report

Use the following command to configure report related settings.

report auto-cache

Use this command to view or configure report auto-cache settings.

Syntax

```
config system report auto-cache
   set aggressive-schedule {enable | disable}
   set order {latest-first | oldest-first}
   set status {enable | disable}
end
```

Variable	Description
aggressive-schedule {enable | disable}	Enable/disable auto-cache on schedule reports aggressively (default = disable).
order {latest-first | oldest-first}	The order of which SQL log table is processed first: • `latest-first`: The newest SQL log table is processed first. • `oldest-first`: The oldest SQL log table is processed first (default).
status {enable | disable}	Enable/disable the SQL report auto-cache (default = enable).

report est-browse-time

Use this command to view or configure report settings.

Syntax

```
config system report est-browse-time
   set max-read-time <integer>
   set status {enable | disable}
end
```

Variable	Description
max-read-time <integer>	Set the read time threshold for each page view (1 - 3600, default = 180).
status {enable | disable}	Enable/disable estimating browse time (default = enable).

report group

Use these commands to configure report groups.

Syntax

```
config system report group
   edit <group-id>
      set adom <adom-name>
      set case-insensitive {enable | disable}
      set report-like <string>
      config chart-alternative
         edit <chart-name>
            set chart-replace <string>
         end
      config group-by
         edit <var-name>
            set var-expression <string>
            set var-type {enum | integer | ip | string}
         end
   end
```

Variable	Description
<group-id>	The identification number of the group to be edited or created.
adom <adom-name>	The ADOM that contains the report group.
case-insensitive {enable | disable}	Enable/disable case sensitivity (default = enable).
report-like <string>	Report pattern
Variables for `config chart-alternative` **subcommand**:	
<chart-name>	The chart name.
chart-replace <string>	Chart replacement.
Variable for `config group-by` **subcommand**:	
<var-name>	The variable name.
var-expression <string>	Variable expression.
var-type {enum | integer | ip | string}	Variable type (default = string).

report setting

Use these commands to view or configure report settings.

Syntax

```
config system report setting
   set aggregate-report {enable | disable}
   set hcache-lossless {enable | disable}
   set ldap-cache-timeout <integer>
   set max-table-rows <integer>
   set report-priority {auto | high | low}
```

```
    set template-auto-install {default}
    set week-start {mon | sun}
end
```

Variable	Description
aggregate-report {enable | disable}	Enable/disable including a group report along with the per-device reports (default = disable).
hcache-lossless {enable | disable}	Enable/disable ready-with-loss hcaches.
ldap-cache-timeout <integer>	Set the LDAP cache timeout in minutes (0 = do not use cache, default = 60).
max-table-rows <integer>	Set the maximum number of rows that can be generated in a single table (10000 - 100000, default = 10000).
report-priority {auto | high | low}	Set the Priority of the SQL report (default = auto).
template-auto-install {default}	Set the language used for new ADOMs (default = default).
week-start {mon | sun}	Set the day that the week starts on, either `sun` (Sunday) or `mon` (Monday) (default = sun).

route

Use this command to view or configure static routing table entries on your FortiAnalyzer unit.

Syntax

```
config system route
   edit <seq_int>
      set device <port>
      set dst <dst_ipv4mask>
      set gateway <gateway_ipv4_address>
   end
```

Variable	Description
<seq_int>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.
device <port>	Enter the port (interface) used for this route.
dst <dst_ipv4mask>	Enter the IPv4 address and mask for the destination network.
gateway <gateway_ipv4_address>	Enter the default gateway IPv4 address for this network.

route6

Use this command to view or configure static IPv6 routing table entries on your FortiAnalyzer unit.

Syntax

```
config system route6
   edit <seq_int>
      set device <string>
      set dst <ipv6_prefix>
      set gateway <ipv6_address>
   end
```

Variable	Description
<seq_int>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.
device <string>	Enter the port (interface) used for this route.
dst <ipv6_prefix>	Enter the IPv4 address and mask for the destination network.
gateway <ipv6_address>	Enter the default gateway IPv6 address for this network.

snmp

Use the following commands to configure SNMP related settings.

snmp community

Use this command to configure SNMP communities on your FortiAnalyzer unit.

You add SNMP communities so that SNMP managers, typically applications running on computers to monitor SNMP status information, can connect to the FortiAnalyzer unit (the SNMP agent) to view system information and receive SNMP traps. SNMP traps are triggered when system events happen such as when there is a system restart, or when the log disk is almost full.

You can add up to three SNMP communities, and each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiAnalyzer unit for a different set of events.

Hosts are the SNMP managers that make up this SNMP community. Host information includes the IPv4 address and interface that connects it to the FortiAnalyzer unit.

For more information on SNMP traps and variables, see the Fortinet Document Library.

Part of configuring an SNMP manager is to list it as a host in a community on the FortiAnalyzer unit that it will be monitoring. Otherwise that SNMP manager will not receive any traps or events from the FortiAnalyzer unit, and will be unable to query the FortiAnalyzer unit as well.

Syntax

```
config system snmp community
   edit <index_number>
      set events <events_list>
      set name <community_name>
      set query-v1-port <integer>
      set query-v1-status {enable | disable}
      set query-v2c-port <integer>
      set query-v2c-status {enable | disable}
      set status {enable | disable}
      set trap-v1-rport <integer>
      set trap-v1-status {enable | disable}
      set trap-v2c-rport <integer>
      set trap-v2c-status {enable | disable}
      config hosts
         edit <host_number>
            set interface <interface_name>
            set ip <ipv4_address>
         end
      config hosts6
         edit <host_number>
            set interface <interface_name>
            set ip <ipv6_address>
         end
   end
```

Variable	Description
<index_number>	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.
events <events_list>	Enable the events for which the FortiManager unit should send traps to the SNMP managers in this community (default = All events enabled). The `raid_changed` event is only available for devices that support RAID. • `cpu-high-exclude-nice`: CPU usage exclude NICE threshold. • `cpu_high`: CPU usage too high. • `disk_low`: Disk usage too high. • `ha_switch`: HA switch. • `intf_ip_chg`: Interface IP address changed. • `lic-dev-quota`: High licensed device quota detected. • `lic-gbday`: High licensed log GB/day detected. • `log-alert`: Log base alert message. • `log-data-rate`: High incoming log data rate detected. • `log-rate`: High incoming log rate detected. • `mem_low`: Available memory is low. • `raid_changed`: RAID status changed. • `sys_reboot`: System reboot.
name <community_name>	Enter the name of the SNMP community. Names can be used to distinguish between the roles of the hosts in the groups.

Variable	Description
	For example the Logging and Reporting group would be interested in the `disk_low` events, but likely not the other events. The name is included in SNMPv2c trap packets to the SNMP manager, and is also present in query packets from, the SNMP manager.
query-v1-port <integer>	Enter the SNMPv1 query port number used when SNMP managers query the FortiManager unit (1 - 65535, default = 161).
query-v1-status {enable | disable}	Enable/disable SNMPv1 queries for this SNMP community (default = enable).
query-v2c-port <integer>	Enter the SNMP v2c query port number used when SNMP managers query the FortiManager unit. SNMP v2c queries will include the name of the community (1 - 65535, default = 161).
query-v2c-status {enable | disable}	Enable/disable SNMPv2c queries for this SNMP community (default = enable).
status {enable | disable}	Enable/disable this SNMP community (default = enable).
trap-v1-rport <integer>	Enter the SNMPv1 remote port number used for sending traps to the SNMP managers (1 - 65535, default = 162).
trap-v1-status {enable | disable}	Enable/disable SNMPv1 traps for this SNMP community (default = enable).
trap-v2c-rport <integer>	Enter the SNMPv2c remote port number used for sending traps to the SNMP managers (1 - 65535, default = 162).
trap-v2c-status {enable | disable}	Enable/disable SNMPv2c traps for this SNMP community. SNMP v2c traps sent out to SNMP managers include the community name (default = enable).
Variables for `config hosts` **subcommand**:	
<host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.
interface <interface_name>	Enter the name of the FortiAnalyzer unit that connects to the SNMP manager (default = any).
ip <ipv4_address>	Enter the IPv4 address of the SNMP manager.
Variables for `config hosts6` **subcommand**:	
<host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.
interface <interface_name>	Enter the name of the FortiAnalyzer unit that connects to the SNMP manager (default = any).
ip <ipv6_address>	Enter the IPv6 address of the SNMP manager.

Example

This example shows how to add a new SNMP community named SNMP_Com1. The default configuration can be used in most cases with only a few modifications. In the example below the community is added, given a name, and then because this community is for an SNMP manager that is SNMP v1 compatible, all v2c functionality is disabled. After the

community is configured the SNMP manager, or host, is added. The SNMP manager IPv4 address is 192.168.20.34 and it connects to the FortiAnalyzer unit internal interface.

```
config system snmp community
   edit 1
   set name SNMP_Com1
   set query-v2c-status disable
   set trap-v2c-status disable
      config hosts
         edit 1
         set interface internal
         set ip 192.168.10.34
         end
   end
```

snmp sysinfo

Use this command to enable the FortiAnalyzer SNMP agent and to enter basic system information used by the SNMP agent. Enter information about the FortiAnalyzer unit to identify it. When your SNMP manager receives traps from the FortiAnalyzer unit, you will know which unit sent the information. Some SNMP traps indicate high CPU usage, log full, or low memory.

For more information on SNMP traps and variables, see the Fortinet Document Library.

Syntax

```
config system snmp sysinfo
   set contact-info <string>
   set description <description>
   set engine-id <string>
   set fortianalyzer-legacy-sysoid <string>
   set location <location>
   set status {enable | disable}
   set trap-cpu-high-exclude-nice-threshold <percentage>
   set trap-high-cpu-threshold <percentage>
   set trap-low-memory-threshold <percentage>
end
```

Variable	Description
contact-info <string>	Add the contact information for the person responsible for this FortiAnalyzer unit (character limit = 255).
description <description>	Add a name or description of the FortiManager unit (character limit = 255).
engine-id <string>	Local SNMP engine ID string (character limit = 24).
fortianalyzer-legacy-sysoid <string>	Enable to switch back to legacy FortiAnalyzer sysObjectOID (default = disable)..
location <location>	Describe the physical location of the FortiAnalyzer unit (character limit = 255).
status {enable | disable}	Enable/disable the FortiAnalyzer SNMP agent (default = disable).

Variable	Description
trap-cpu-high-exclude-nice-threshold <percentage>	SNMP trap for CPU usage threshold (excluding NICE processes), in percent (default = 80).
trap-high-cpu-threshold <percentage>	SNMP trap for CPU usage threshold, in percent (default = 80).
trap-low-memory-threshold <percentage>	SNMP trap for memory usage threshold, in percent (default = 80).

Example

This example shows how to enable the FortiAnalyzer SNMP agent and add basic SNMP information.

```
config system snmp sysinfo
   set status enable
   set contact-info 'System Admin ext 245'
   set description 'Internal network unit'
   set location 'Server Room A121'
end
```

snmp user

Use this command to configure SNMPv3 users on your FortiAnalyzer unit. To use SNMPv3, you will first need to enable the FortiAnalyzer SNMP agent. For more information, see snmp sysinfo. There should be a corresponding configuration on the SNMP server in order to query to or receive traps from FortiAnalyzer.

For more information on SNMP traps and variables, see the Fortinet Document Library.

Syntax

```
config system snmp user
   edit <name>
      set auth-proto {md5 | sha}
      set auth-pwd <passwd>
      set events <events_list>
      set notify-hosts <ipv4_address>
      set notify-hosts6 <ipv6_address>
      set priv-proto {aes | des}
      set priv-pwd <passwd>
      set queries {enable | disable}
      set query-port <integer>
      set security-level {auth-no-priv | auth-priv | no-auth-no-priv}
   end
end
```

Variable	Description
<name>	Enter a SNMPv3 user name to add, edit, or delete.

Variable	Description
auth-proto {md5 | sha}	Authentication protocol. The security level must be set to `auth-no-priv` or `auth-priv` to use this variable: • `md5`: HMAC-MD5-96 authentication protocol • `sha`: HMAC-SHA-96 authentication protocol (default)
auth-pwd <passwd>	Password for the authentication protocol. The security level must be set to `auth-no-priv` or `auth-priv` to use this variable.
events <events_list>	Enable the events for which the FortiAnalyzer unit should send traps to the SNMPv3 managers in this community (default = All events enabled). The `raid_changed` event is only available for devices which support RAID. • `cpu-high-exclude-nice`: CPU usage exclude nice threshold. • `cpu_high`: The CPU usage is too high. • `disk_low`: The log disk is getting close to being full. • `ha_switch`: A new unit has become the HA master. • `intf_ip_chg`: An interface IP address has changed. • `lic-dev-quota`: High licensed device quota detected. • `lic-gbday`: High licensed log GB/Day detected. • `log-alert`: Log base alert message. • `log-data-rate`: High incoming log data rate detected. • `log-rate`: High incoming log rate detected. • `mem_low`: The available memory is low. • `raid_changed`: RAID status changed. • `sys_reboot`: The FortiAnalyzer unit has rebooted.
notify-hosts <ipv4_address>	Hosts to send notifications (traps) to.
notify-hosts6 <ipv6_address>	Hosts to send notifications (traps) to.
priv-proto {aes | des}	Privacy (encryption) protocol. The security level must be set to `auth-no-priv` or `auth-priv` to use this variable: • `aes`: CFB128-AES-128 symmetric encryption protocol (default) • `des`: CBC-DES symmetric encryption protocol
priv-pwd <passwd>	Password for the privacy (encryption) protocol. The security level must be set to `auth-no-priv` or `auth-priv` to use this variable.
queries {enable | disable}	Enable/disable queries for this user (default = enable)
query-port <integer>	SNMPv3 query port (1 - 65535, default = 161).
security-level {auth-no-priv | auth-priv | no-auth-no-priv}	Security level for message authentication and encryption: • `auth-no-priv`: Message with authentication but no privacy (encryption). • `auth-priv`: Message with authentication and privacy (encryption). • `no-auth-no-priv`: Message with no authentication and no privacy (encryption) (default).

sql

Configure Structured Query Language (SQL) settings.

Syntax

```
config system sql
   set background-rebuild {enable | disable}
   set database-name <string>
   set database-type <postgres>
   set device-count-high {enable | disable}
   set event-table-partition-time <integer>
   set fct-table-partition-time <integer>
   set logtype {none | app-ctrl | attack | content | dlp | emailfilter | event | generic |
        history | traffic | virus | voip | webfilter | netscan}
   set password <passwd>
   set prompt-sql-upgrade {enable | disable}
   set rebuild-event {enable | disable}
   set rebuild-event-start-time <hh:mm> <yyyy/mm/dd>
   set server <string>
   set start-time <hh>:<mm> <yyyy>/<mm>/<dd>
   set status {disable | local | remote}
   set text-search-index {enable | disable}
   set traffic-table-partition-time <integer>
   set utm-table-partition-time <integer>
   set username <string>
   config custom-index
      edit <id>
         set case-sensitive {enable | disable}
         set device-type {FortiCache | FortiGate | FortiMail | FortiSandbox | FortiWeb}
         set index-field <Field-Name>
         set log-type <Log-Enter>
      end
   config ts-index-field
      edit <category>
         set <value> <string>
      end
end
```

Variable	Description
background-rebuild {enable | disable}	Disable/enable rebuilding the SQL database in the background (default = enable).
database-name <string>	Remote SQL database name (character limit = 64).
database-type <postgres>	Database type (default = postgres).
device-count-high {enable | disable}	Enable/disable a high device count (default = disable). You must set to enable if the count of registered devices is greater than 8000: • `disable`: Set to disable if device count is less than 8000. • `enable`: Set to enable if device count is equal to or greater than 8000.

Variable	Description
	Caution: Enabling or disabling this command will result in an SQL database rebuild. The time required to rebuild the database is dependent on the size of the database. Please plan a maintenance window to complete the database rebuild. This operation will also result in a device reboot.
event-table-partition-time <integer>	Maximum SQL database table partitioning time range for event logs, in minutes (0 - 525600, 0 = unlimited, default = 0).
fct-table-partition-time <integer>	Maximum SQL database table partitioning time range for FortiClient logs, in minutes (0 - 525600, 0 = unlimited, default = 240).
logtype {none | app-ctrl | attack | content | dlp | emailfilter | event | generic | history | traffic | virus | voip | webfilter | netscan}	Log type.
password <passwd>	The password that the Fortinet unit will use to authenticate with the remote database.
prompt-sql-upgrade {enable | disable}	Prompt to convert log database into SQL database at start time on GUI (default = enable).
rebuild-event {enable | disable}	Enable/disable a rebuild event during SQL database rebuilding (default = enable).
rebuild-event-start-time <hh:mm> <yyyy/mm/dd>	The rebuild event starting date and time (default = 00:00 2000/01/01).
server <string>	Set the database ip or hostname.
start-time <hh>:<mm> <yyyy>/<mm>/<dd>	The date and time that logs will start to be inserted.
status {disable | local | remote}	SQL database status: • `disable`: Disable SQL database. • `local`: Enable local database (default). • `remote`: Enable remote database.
text-search-index {enable | disable}	Enable/disable the creation of a text search index (default = disable).
traffic-table-partition-time <integer>	Maximum SQL database table partitioning time range for traffic logs (0 - 525600, 0 = unlimited, default = 0).
utm-table-partition-time <integer>	Maximum SQL database table partitioning time range in minutes for UTM logs (0 - 525600, 0 = unlimited, default = 0).
username <string>	The user name that the unit will use to authenticate with the remote database (character limit = 64).
Variables for `config custom-index` **subcommand**:	
case-sensitive {enable | disable}	Enable/disable case sensitivity.

<table>
<tr><th>Variable</th><th>Description</th></tr>
<tr><td>device-type {FortiAuthenticator | FortiCache | FortiClient | FortiDDoS | FortiGate | FortiMail | FortiManager | FortiSandbox | FortiWeb}</td><td>Set the device type (default = FortiGate).</td></tr>
<tr><td>index-field <Field-Name></td><td>Enter a valid field name. Select one of the available field names. The available options for <code>index-field</code> is dependent on the <code>device-type</code> entry.</td></tr>
<tr><td>log-type <Log-Enter></td><td>Enter the log type. The available options for <code>log-type</code> is dependent on the <code>device-type</code> entry.</td></tr>
<tr><td colspan="2">Variables for <code>config ts-index-field</code> subcommand:</td></tr>
<tr><td><category></td><td>Category of the text search index fields. The following is the list of categories and their default fields.
<table>
<tr><th>Category</th><th>Value</th></tr>
<tr><td>FGT-app-ctrl</td><td>user,group,srcip,dstip,dstport,service,app,action,hostname</td></tr>
<tr><td>FGT-attack</td><td>severity,srcip,dstip,action,user,attack</td></tr>
<tr><td>FGT-content</td><td>from,to,subject,action,srcip,dstip,hostname,status</td></tr>
<tr><td>FGT-dlp</td><td>user,srcip,service,action,filename</td></tr>
<tr><td>FGT-emailfilter</td><td>user,srcip,from,to,subject</td></tr>
<tr><td>FGT-event</td><td>subtype,ui,action,msg</td></tr>
<tr><td>FGT-traffic</td><td>user,srcip,dstip,service,app,utmaction</td></tr>
<tr><td>FGT-virus</td><td>service,srcip,dstip,action,filename,virus,user</td></tr>
<tr><td>FGT-voip</td><td>action,user,src,dst,from,to</td></tr>
<tr><td>FGT-webfilter</td><td>user,srcip,dstip,service,action,catdesc,hostname</td></tr>
<tr><td>FGT-netscan</td><td>user,dstip,vuln,severity,os</td></tr>
<tr><td>FGT-fct-event</td><td>(null)</td></tr>
<tr><td>FGT-fct-traffic</td><td>(null)</td></tr>
<tr><td>FGT-fct-netscan</td><td>(null)</td></tr>
<tr><td>FGT-waf</td><td>user,srcip,dstip,service,action</td></tr>
<tr><td>FGT-gtp</td><td>msisdn,from,to,status</td></tr>
<tr><td>FGT-dns</td><td>(null)</td></tr>
<tr><td>FGT-ssh</td><td>login,srcip,dstip,direction,action</td></tr>
<tr><td>FML-emailfilter</td><td>client_name,dst_ip,from,to,subject</td></tr>
</table></td></tr>
</table>

Variable	Description	
	Category	Value
	FML-event	subtype,msg
	FML-history	classifier,disposition,from,to,client_name,direction,domain,virus
	FML-virus	src,msg,from,to
	FWB-attack	http_host,http_url,src,dst,msg,action
	FWB-event	ui,action,msg
	FWB-traffic	src,dst,service,http_method,msg
value <string>	Fields of the text search filter. Enter one or more field names separated with a comma.	

syslog

Use this command to configure syslog servers.

Syntax

```
config system syslog
   edit <name>
      set ip <string>
      set port <integer>
   end
end
```

Variable	Description
<name>	Syslog server name.
ip <string>	Enter the syslog server IPv4 address or hostname.
port <integer>	Enter the syslog server port (1 - 65535, default = 514).

workflow approval-matrix

Use this command to configure workflow settings.

Syntax

```
config system workflow approval-matrix
```

```
    edit <ADOM_name>
       set mail-server <string>
       set notify <string>
       config approver
          edit <sequence_number>
          set member <string>
    end
end
```

Variable	Description
<ADOM_name>	The name of the ADOM.
mail-server <string>	Enter the mail server IPv4 address or hostname.
notify <string>	Enter the notified users. Use a comma as a separator.
Variables for `config approver` **subcommand**:	
<sequence_number>	Enter the entry number.
member <string>	Enter the members of the approval group. Use a comma as a separator.

Example

This example shows configuring the `admin` administrator as an approver for the `root` ADOM.

```
config system workflow approval-matrix
   edit "root"
      config approver
         edit 1
            set member "admin"
         next
      end
   set mail-server "mail.fortinet.com"
   set notify "admin"
end
```

fmupdate

Use `fmupdate` to configure settings related to FortiGuard service updates and the FortiAnalyzer unit's built-in FortiGuard Distribution Server (FDS).

CLI commands and variables are case sensitive.

analyzer virusreport

Use this command to enable or disable notification of virus detection to Fortinet.

Syntax

```
config fmupdate analyzer virusreport
   set status {enable | disable}
end
```

Variables	Description
status {enable | disable}	Enable/disable sending virus detection notification to FortiGuard (default = enable).

Example

This example enables virus detection notifications to Fortinet.

```
config fmupdate analyzer virusreport
   set status enable
end
```

av-ips

Use the following commands to configure antivirus settings.

av-ips advanced-log

Use this command to enable logging of FortiGuard Antivirus and IPS update packages received by the FortiAnalyzer unit's built-in FDS from the FortiGuard Distribution Network (FDN).

Syntax

```
config fmupdate av-ips advanced-log
   set log-fortigate {enable | disable}
   set log-server {enable | disable}
end
```

Variables	Description
log-fortigate {enable | disable}	Enable/disable logging of FortiGuard antivirus and IPS service updates of FortiGate devices (default = disable).
log-server {enable | disable}	Enable/disable logging of update packages received by the built-in FDS server (default = enable).

Example

Enable logging of FortiGuard Antivirus updates to FortiClient installations and update packages downloaded by the built-in FDS from the FDN.

```
config fmupdate av-ips advanced-log
   set log-forticlient enable
   set log-server enable
end
```

av-ips web-proxy

Use this command to configure a web proxy if FortiGuard Antivirus and IPS updates must be retrieved through a web proxy.

Syntax

```
config fmupdate av-ips web-proxy
   set ip <ipv4_address>
   set ip6 <ipv6_address>
   set mode {proxy | tunnel}
   set password <password>
   set port <integer>
   set status {enable | disable}
```

```
    set username <string>
end
```

Variables	Description
ip <ipv4_address>	Enter the IPv4 address of the web proxy.
ip6 <ipv6_address>	Enter the IPv6 address of the web proxy.
mode {proxy | tunnel}	Enter the web proxy mode (default = proxy).
password <password>	If the web proxy requires authentication, enter the password for the user name (character limit = 63).
port <integer>	Enter the port number of the web proxy (1 - 65535, default = 80).
status {enable | disable}	Enable/disable connections through the web proxy (default = disable).
username <string>	If the web proxy requires authentication, enter the user name (character limit = 63).

Example

You could enable a connection through a non-transparent web proxy on an alternate port.

```
config fmupdate av-ips web-proxy
    set status enable
    set mode proxy
    set ip 10.10.30.1
    set port 8890
    set username avipsupdater
    set password cvhk3rf3u9jvsYU
end
```

custom-url-list

Use this command to configure the URL database for rating and filtering. You can select to use the FortiGuard URL database, a custom URL database, or both. When selecting to use a custom URL database, use the `fmupdate {ftp | scp | tftp} import` command to import the custom URL list. When FortiAnalyzer performs the URL rating, it will check the custom URL first. If a match is found, the custom rating is returned. If there is no match, then FortiAnalyzer will check the FortiGuard database.

Syntax

```
config fmupdate custom-url-list
    set db_selection {both | custom-url | fortiguard-db}
end
```

Variable	Description
db_selection {both | custom-url | fortiguard-db}	Manage the FortiGuard URL database: • `both`: Support both custom URL database and the FortiGuard database (default) • `custom-url`: Customer imported URL list. • `fortiguard-db`: Fortinet's FortiGuard database

disk-quota

Use this command to configure the disk space available for use by the Upgrade Manager.

If the Upgrade Manager disk space is full or if there is insufficient space to save an update package to disk, the package will not download and an alert will be sent to notify you.

Syntax

```
config fmupdate disk-quota
   set value <size_int>
end
```

Variable	Description
value <size_int>	Configure the size of the Upgrade Manager disk quota, in megabytes (default = 51200). If you set the disk-quota smaller than the size of an update package, the update package will not download and you will get a disk full alert.

fct-services

Use this command to configure the built-in FDS to provide FortiGuard services to FortiClient installations.

Syntax

```
config fmupdate fct-services
   set status {enable | disable}
   set port <port_int>
end
```

Variables	Description
status {enable | disable}	Enable/disable built-in FDS service to FortiClient installations (default = enable).
port <port_int>	Enter the port number on which the built-in FDS should provide updates to FortiClient installations (1 - 65535, default = 80).

Example

You could configure the built-in FDS to accommodate older versions of FortiClient installations by providing service on their required port.

```
config fmupdate fct-services
   set status enable
   set port 80
end
```

fds-setting

Use this command to set FDS settings.

Syntax

```
config fmupdate fds-settings
   set fds-clt-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}
   set fds-ssl-protocol
   set fmtr-log {alert | critical | debug | disable | emergency | error | info | notice |
        warn}
   set linkd-log {alert | critical | debug | disable | emergency | error | info | notice |
        warn}
   set max-av-ips-version <integer>
   set max-work <integer>
   set send_report {enable | disable}
   set send_setup {enable | disable}
   set system-support-faz {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
   set system-support-fct {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
   set system-support-fgt {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
   set system-support-fml {4.x | 5.x}
   set system-support-fsa {1.x | 2.x}
   set system-support-fsw {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}
   set umsvc-log {alert | critical | debug | disable | emergency | error | info | notice |
        warn}
   set unreg-dev-option {add-service | ignore | svc-only}
   set User-Agent <text>
end
```

Variables	Description
fds-clt-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}	Set the SSL protocols version for connecting FDS server (default = tlsv1.2).
fds-ssl-protocol {sslv3 | tlsv1.0 | tlsv1.1 | tlsv1.2}	Set the SSL protocols version for FDS service (default = tlsv1.0).
fmtr-log {alert | critical | debug | disable | emergency | error | info | notice | warn}	The fmtr log level. Set to `disable` to disable the log (default = info).

Variables	Description
linkd-log {alert | critical | debug | disable | emergency | error | info | notice | warn}	The linkd log level (default = info).
max-av-ips-version <integer>	The maximum number of AV/IPS full version downloadable packages (default = 20).
max-work <integer>	The maximum number of worker processing downlink requests (default = 1).
send_report {enable | disable}	Enable/disable sending reports to the FDS server (default = disable).
send_setup {enable | disable}	Enable/disable sending setup to the FDS server (default = disable).
system-support-faz {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}	Set the FortiAnalyzer support version (default = 5.0 5.2 5.4 5.6 6.0).
system-support-fct {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}	Set the FortiClient support version.
system-support-fgt {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}	Set the FortiGate support version.
system-support-fml {4.x | 5.x}	Set the FortiMail support version.
system-support-fsa {1.x | 2.x}	Set the FortiSandbox support version.
system-support-fsw {4.x | 5.0 | 5.2 | 5.4 | 5.6 | 6.0}	Set the FortiSwitch support version.
umsvc-log {alert | critical | debug | disable | emergency | error | info | notice | warn}	The um_service log level (default = info).
unreg-dev-option {add-service | ignore | svc-only}	Set the option for unregistered devices: • `add-service`: Add unregistered devices and allow update request (default). • `ignore`: Ignore all unregistered devices. • `svc-only`: Allow update request without add unregistered device.
User-Agent <text>	Configure the User-Agent string.

fds-setting push-override

Use this command to enable or disable push updates, and to override the default IP address and port to which the FDS sends FortiGuard antivirus and IPS push messages.

This is useful if push notifications must be sent to an IP address and/or port other than the FortiAnalyzer unit, such as the external or virtual IP address of a NAT device that forwards traffic to the FortiAnalyzer unit.

Syntax

```
config fmupdate fds-setting
   config push-override
```

```
      set ip <ipv_address>
      set port <integer>
      set status {enable | disable}
   end
end
```

Variable	Description
ip <ipv_address>	Enter the external or virtual IP address of the NAT device that will forward push messages to the FortiAnalyzer unit.
port <integer>	Enter the receiving port number on the NAT device (1 - 65535, default = 9443).
status {enable | disable}	Enable/disable the push updates (default = disable).

Example

You could enable the FortiAnalyzer unit's built-in FDS to receive push messages.

If there is a NAT device or firewall between the FortiAnalyzer unit and the FDS, you could also notify the FDS to send push messages to the external IP address of the NAT device, instead of the FortiAnalyzer unit's private network IP address.

```
config fmupdate fds-setting
   config push-override
      set status enable
      set ip 172.16.124.135
      set port 9000
   end
end
```

You would then configure port forwarding on the NAT device, forwarding push messages received on User Datagram Protocol (UDP) port 9000 to the FortiAnalyzer unit on UDP port 9443.

fds-setting push-override-to-client

Use this command to enable or disable push updates, and to override the default IP address and port to which the FDS sends FortiGuard antivirus and IPS push messages.

This command is useful if push notifications must be sent to an IP address and/or port other than the FortiAnalyzer unit, such as the external or virtual IP address of a NAT device that forwards traffic to the FortiAnalyzer unit.

Syntax

```
config fmupdate fds-setting
   config push-override-to-client
      set status {enable | disable}
      config <announce-ip>
         edit <id>
            set ip <ip_address>
            set port <integer>
      end
   end
end
```

Variable	Description
status {enable | disable}	Enable/disable the push updates (default = disable).
Variables for `config announce-ip` **subcommand**:	
<id>	Edit the announce IP address ID (1 - 10).
ip <ip_address>	Enter the announce IP address.
port <integer>	Enter the announce IP port (1 - 65535, default = 8890).

fds-setting server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard spam updates.

Syntax

```
config fmupdate fds-setting
   config server-override
      set status {enable | disable}
      config servlist
         edit <id>
            set ip <ipv4_address>
            set ip6 <ipv6_address>
            set port <integer>
            set server-type {fct | fds}
      end
   end
end
```

Variable	Description
status {enable | disable}	Enable/disable the override (default = disable).
Variable for `config servlist` **subcommand**:	
<id>	Enter the override server ID (1 - 10).
ip <ipv4_address>	Enter the IPv4 address of the override server address.
ip6 <ipv6_address>	Enter the IPv6 address of the override server address.
port <integer>	Enter the port number to use when contacting the FDS (1 - 65535, default = 443).
server-type {fct| fds}	Set the override server type (default = fds).

fds-setting update-schedule

Use this command to schedule when the built-in FortiGuard retrieves antivirus and IPS updates.

Syntax

```
config fmupdate fds-setting
   config update-schedule
      set day {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday}
      set frequency {every | daily | weekly}
      set status {enable | disable}
      set time <hh:mm>
   end
end
```

Variable	Description
day {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday}	The day that the update will occur (Sunday - Saturday, default = Monday). This option is only available if the update frequency is `weekly`.
frequency {every | daily | weekly}	The update frequency: every given time interval, once a day, or once a week (default = every).
status {enable | disable}	Enable/disable scheduled updates (default = enable).
time <hh:mm>	The time interval between updates, or the hour and minute when the update occurs (hh: 0 - 23, mm: 0 - 59 or 60 = random, default = 00:10).

multilayer

Use this command to set multilayer mode configuration.

Syntax

```
config fmupdate multilayer
   set webspam-rating {enable | disable}
end
```

Variables	Description
webspam-rating {enable | disable}	Enable/disable URL/antispam rating service (default = enable).

publicnetwork

Use this command to enable access to the public FDS. If this function is disabled, the service packages, updates, and license upgrades must be imported manually.

Syntax

```
config fmupdate publicnetwork
   set status {enable | disable}
end
```

Variables	Description
status {enable | disable}	Enable/disable the public network (default = enable).

server-access-priorities

Use this command to configure how a FortiGate unit may download antivirus updates and request web filtering services from multiple FortiAnalyzer units and private FDS servers.

Use the `private-server` subcommand to configure multiple FortiAnalyzer units and private servers.

By default, the FortiGate unit receives updates from the FortiAnalyzer unit if the FortiGate unit is managed by the FortiAnalyzer unit and the FortiGate unit was configured to receive updates from the FortiAnalyzerunit.

Syntax

```
config fmupdate server-access-priorities
   set access-public {enable | disable}
   set av-ips {enable | disable}
   set web-spam {enable | disable}
   config private-server
      edit <id>
         set ip <ipv4_address>
         set ip6 <ipv6_address>
         set time_zone <integer>
      end
   end
```

Variables	Description
access-public {enable | disable}	Enable/disable allowing FortiGates to access public FortiGuard servers when private servers are unavailable (default = disable).
av-ips {enable | disable}	Enable/disable receiving antivirus and IPS update service for private servers (default = disable).
web-spam {enable | disable}	Enable/disable Web Filter and Email Filter update service for private servers (default = enable).
Variables for `config private-server` **subcommand**:	
<id>	Enter a number to identify the FortiManager unit or private server (1 - 10).

Variables	Description
ip <ipv4_address>	Enter the IPv4 address of the FortiManager unit or private server.
ip6 <ipv6_address>	Enter the IPv6 address of the FortiManager unit or private server.
time_zone <integer>	Enter the correct time zone of the private server (-24 = local time zone, default = -24).

Example

The following example configures access to public FDS servers and allows FortiGate units to receive antivirus updates from other FortiAnalyzer units and private FDS servers. This example also configures two private servers.

```
config fmupdate server-access-priorities
   set access-public enable
   set av-ips enable
      config private-server
         edit 1
            set ip 172.16.130.252
         next
         edit 2
            set ip 172.31.145.201
         end
      end
```

server-override-status

Configure strict or loose server override.

Syntax

```
config fmupdate server-override-status
   set mode {loose | strict}
end
```

Variables	Description
mode {loose | strict}	Set the server override mode: • `loose`: Allow access other servers (default). • `strict`: Access override server only.

service

Use this command to enable or disable the services provided by the built-in FDS.

Syntax

```
config fmupdate service
   set avips {enable | disable}
   set query-geoip {enable | disable}
end
```

Variables	Description
avips {enable | disable}	Enable/disable the built-in FortiGuard to provide FortiGuard antivirus and IPS updates (default = enable).
query-geoip {enable | disable}	Enable/disable geoip service (default = enable).

Example

```
config fmupdate service
   set avips enable
end
```

web-spam

Use the following commands to configure FortiGuard antispam related settings.

web-spam fgd-setting

Use this command to configure FortiGuard run parameters.

Syntax

```
config fmupdate web-spam fgd-setting
   set as-cache <integer>
   set as-log {all | disable | nospam}
   set as-preload {enable | disable}
   set av-cache <integer>
   set av-log {all | disable | novirus}
   set av-preload {enable | disable}
   set eventlog-query {enable | disable}
   set fgd-pull-interval <integer>
   set fq-cache <integer>
   set fq-log {all | disable | nofilequery}
   set fq-preload {enable | disable}
   set linkd-log {enable | disable}
   set max-log-quota <integer>
   set max-unrated-size <integer>
   set restrict-as1-dbver <string>
   set restrict-as2-dbver <string>
   set restrict-as4-dbver <string>
   set restrict-av-dbver <string>
```

```
    set restrict-fq-dbver <string>
    set restrict-wf-dbver <string>
    set stat-log-interval <integer>
    set stat-sync-interval <integer>
    set update-interval <integer>
    set update-log {enable | disable}
    set wf-cache <integer>
    set wf-dn-cache-expire-time <integer>
    set wf-dn-cache-max-number <integer>
    set wf-log {all | disable | nourl}
    set wf-preload {enable | disable}
    config server-override
       set status {enable | disable}
       config servlist
          edit <id>
             set ip <ipv4_address>
             set ip6 <ipv6_address>
             set port <integer>
             set service-type {fgc | fgd | fsa}
       end
    end
end
```

Variable	Description
as-cache <integer>	Antispam service maximum memory usage in megabytes (Maximum = Physical memory-1024, 0 = no limit, default = 300).
as-log {all | disable | nospam}	Antispam log setting: • `all`: Log all spam lookups. • `disable`: Disable spam log. • `nospam`: Log non-spam events (default)
as-preload {enable | disable}	Enable/disable preloading the antispam database into memory (default = disable).
av-cache <integer>	Antivirus service maximum memory usage, in megabytes (100 - 500, default = 300).
av-log {all | disable | novirus}	Antivirus log setting: • `all`: Log all virus lookups. • `disable`: Disable virus log. • `novirus`: Log non-virus events (default).
av-preload {enable | disable}	Enable/disable preloading antivirus database to memory (default = disable).
eventlog-query {enable | disable}	Enable/disable record query to event-log besides fgd-log (default = disable).
fgd-pull-interval <integer>	FortiGuard pull interval setting, in minutes (1 - 1440, default = 10).
fq-cache <integer>	File query service maximum memory usage, in megabytes (100 - 500, default = 300).
fq-log {all | disable | nofilequery}	Filequery log setting: • `all`: Log all file query. • `disable`: Disable file query log.

Variable	Description
	• `nofilequery`: Log non-file query events (default).
fq-preload {enable | disable}	Enable/disable preloading the filequery database to memory (default = disable).
linkd-log {enable | disable}	Linkd log setting: • `alert`: Immediate action is required. • `critical`: Functionality is affected. • `debug`: Debug information (default). • `disable`: Linkd logging is disabled. • `emergency`: The unit is unusable. • `error`: Functionality is probably affected. • `info`: General information. • `notice`: Information about normal events. • `warn`: Functionality might be affected.
max-log-quota <integer>	Maximum log quota setting, in megabytes (100 - 20480, default = 6144).
max-unrated-size <integer>	Maximum number of unrated site in memory, in kilobytes(10 - 5120, default = 500).
restrict-as1-dbver <string>	Restrict system update to indicated antispam(1) database version (character limit = 127).
restrict-as2-dbver <string>	Restrict system update to indicated antispam(2) database version (character limit = 127).
restrict-as4-dbver <string>	Restrict system update to indicated antispam(4) database version (character limit = 127).
restrict-av-dbver <string>	Restrict system update to indicated antivirus database version (character limit = 127).
restrict-fq-dbver <string>	Restrict system update to indicated file query database version (character limit = 127).
restrict-wf-dbver <string>	Restrict system update to indicated web filter database version (character limit = 127).
stat-log-interval <integer>	Statistic log interval setting, in minutes (1 - 1440, default = 60).
stat-sync-interval <integer>	Synchronization interval for statistic of unrated site in minutes (1 - 60, default = 60).
update-interval <integer>	FortiGuard database update wait time if not enough delta files, in hours (2 - 24, default = 6).
update-log {enable | disable}	Enable/disable update log setting (default = enable).
wf-cache <integer>	Web filter service maximum memory usage, in megabytes (maximum = Physical memory-1024, 0 = no limit, default = 600).
wf-dn-cache-expire-time	Web filter DN cache expire time, in minutes (1 - 1440, 0 = never, default = 30).
wf-dn-cache-max-number	Maximum number of Web filter DN cache (0 = disable, default = 10000).

Variable	Description
wf-log {all | disable | nourl}	Web filter log setting: • `all`: Log all URL lookups. • `disable`: Disable URL log. • `nourl`: Log non-URL events (default).
wf-preload {enable | disable}	Enable/disable preloading the web filter database into memory (default = disable).
Variables for `config server-override` **subcommand**:	
status {enable | disable}	Enable/disable the override (default = disable).
<id>	Override server ID (1 - 10).
ip <ipv4_address>	IPv4 address of the override server.
ip6 <ipv6_address>	IPv6 address of the override server.
port <integer>	Port number to use when contacting FortiGuard (1 - 65535, default = 443).
service-type {fgc | fgd | fsa}	Override service type.

web-spam web-proxy

Use this command to configure the web-spam web-proxy.

Syntax

```
config fmupdate web-spam web-proxy
   set ip <proxy_ipv4_address>
   set ip6 <proxy_ipv6_address>
   set mode {proxy | tunnel}
   set password <passwd>
   set port <integer>
   set status {enable | disable}
end
```

Variable	Description
ip <proxy_ipv4_address>	Enter the IPv4 address of the web proxy.
ip6 <proxy_ipv6_address>	Enter the IPv6 address of the web proxy.
mode {proxy | tunnel}	Enter the web proxy mode (default = proxy).
password <passwd>	If the web proxy requires authentication, type the password for the user name.
port <integer>	Enter the port number of the web proxy (1- 65535, default = 80).
status {enable | disable}	Enable/disable connections through the web proxy (default = disable).
username <string>	If the web proxy requires authentication, enter the user name.

execute

The `execute` commands perform immediate operations on the FortiAnalyzer unit. You can:

- Back up and restore the system settings, or reset the unit to factory settings.
- Set the unit date and time.
- Use ping to diagnose network problems.
- View the processes running on the FortiAnalyzer unit.
- Start and stop the FortiAnalyzer unit.
- Reset or shut down the FortiAnalyzer unit.

FortiAnalyzer CLI commands and variables are case sensitive.

add-mgmt-license	fmupdate	ping	sql-query-dataset
add-vm-license	format	ping6	sql-query-generic
backup	iotop	raid	sql-report
bootimage	iotps	reboot	ssh
certificate	log	remove	ssh-known-hosts
console	log-aggregation	reset	tac
date	log-fetch	restore	time
device	log-integrity	sensor	top
erase-disk	lvm	shutdown	traceroute
factory-license	migrate	sql-local	traceroute6

add-mgmt-license

Use this command to load management licenses to the FortiAnalyzer.

This command is only available on hardware-based FortiAnalyzer models.

Syntax

```
execute add-mgmt-license <mgmt license string>
```

Variable	Description
<mgmt license string>	The license string. Copy and paste the string from the license file. The license string must be enclosed with double quotes. Do not removed line breaks from the string.

Example

The contents of the license file needs to be in quotes in order for it to work.

```
execute add-mgmt-license "-----BEGIN FAZ MGMT LICENSE-----
QAAAAJ09s+LTe...ISJTTYPcKoDmMa6
-----END FAZ MGMT LICENSE-----"
```

add-vm-license

Add a VM license to the FortiAnalyzer.

Syntax

```
execute add-vm-license <vm license string>
```

Variable	Description
<vm license string>	The VM license string. Copy and paste the string from the license file. The license string must be enclosed with double quotes. Do not removed line breaks from the string.

Example

The contents of the license file needs to be in quotes in order for it to work.

```
execute add-vm-license "-----BEGIN FAZ VM LICENSE-----
QAAAAJ09s+LTe...ISJTTYPcKoDmMa6
-----END FAZ VM LICENSE-----"
```

This command is only available on FortiAnalyzer VM models.

backup

Use the following commands to backup all settings or logs on your FortiAnalyzer.

When you back up the unit settings from the vdom_admin account, the backup file contains global settings and the settings for each VDOM. When you back up the unit settings from a regular administrator account, the backup file contains the global settings and only the settings for the VDOM to which the administrator belongs.

Syntax

```
execute backup all-settings {ftp | scp | sftp} <ip:port> <string> <username> <passwd> <ssh-
    cert> [crptpasswd]
execute backup logs <device name(s)> {ftp | scp | sftp} <ip> <username> <passwd> <directory>
    [vdlist]
execute backup logs-only <device name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
    <directory> [vdlist]
execute backup logs-rescue <device serial number(s)> {ftp | scp | sftp} <ip> <username>
    <passwd> <directory> [vdlist]
execute backup reports <report schedule name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
    <directory> [vdlist]
execute backup reports-config <adom name(s)> {ftp | scp | sftp} <ip> <username> <passwd>
    <directory> [vdlist]
```

Variable	Description
all-settings	Backup all FortiAnalyzer settings to a file on a server.
logs	Backup the device logs to a specified server.
logs-only	Backup device logs only to a specified server.
logs-rescue	Use this hidden command to backup logs regardless of DVM database for emergency reasons. This command will scan folders under /Storage/Logs/ for possible device logs to backup.
reports	Backup the reports to a specified server.
reports-config	Backup reports configuration to a specified server.
<device name(s)>	Enter the device name(s) separated by a comma, or enter `all` for all devices.
<device serial number(s)>	Enter the device serial number(s) separated by a comma, or enter `all` for all devices.
<report schedule name(s)>	Enter the report schedule name(s) separated by a comma, or enter `all` for all reports schedules.
<adom name(s)>	Enter the ADOM name(s) separated by a comma, or enter `all` for all ADOMs.
{ftp | scp | sftp}	Enter the server type: `ftp`, `scp`, or `sftp`.
<ip:port>	Enter the server IP address and optionally , for FTP servers, the port number.
<ip>	Enter the server IP address.

Variable	Description
<string>	Enter the path and file name for the backup.
<username>	Enter username to use to log on the backup server.
<passwd>	Enter the password for the username on the backup server.
<ssh-cert>	Enter the SSH certification for the server. This option is only available for backup operations to SCP servers.
[crptpasswd]	Optional password to protect backup content. Use `any` for no password.
<directory>	Enter the path to where the file will be backed up to on the backup server.
[vdlist]	VD name(s), separated by commas.

Example

This example shows how to backup the FortiAnalyzer unit system settings to a file named `fmg.cfg` on a server at IP address 192.168.1.23 using the admin username, and password 123457.

```
execute backup all-settings ftp 192.168.1.23 fmd.cfg admin 123457
Starting backup all settings...
Starting transfer the backup file to FTP server...
```

bootimage

Set the image from which the FortiAnalyzer unit will boot the next time it is restarted.

This command is only available on hardware-based FortiAnalyzer models.

Syntax

```
execute bootimage {primary | secondary}
```

Variable	Description
{primary | secondary}	Select to boot from either the primary or secondary partition.

If you do not specify primary or secondary, the command will report whether it last booted from the primary or secondary boot image.

If your FortiAnalyzer unit does not have a secondary image, the bootimage command will inform you that option is not available.

To reboot your FortiAnalyzer unit, use:

```
execute reboot
```

certificate

Use these commands to manage certificates.

certificate ca

Use these commands to list CA certificates, and to import or export CA certificates.

Syntax

To list the CA certificates installed on the FortiAnalyzer unit:

```
execute certificate ca list
```

To export or import CA certificates:

```
execute certificate ca {<export>|<import>} <cert_name> <tftp_ip>
```

Variable	Description
list	Generate a list of CA certificates on the FortiAnalyzer system.
<export>	Export CA certificate to TFTP server.
<import>	Import CA certificate from a TFTP server.
<cert_name>	Name of the certificate.
<tftp_ip>	IP address of the TFTP server.

certificate local

Use these commands to list, import, or export local certificates, and to generate a certificate request

Syntax

```
execute certificate local export <cert_name> <tftp_ip>
execute certificate local import <cert_name> <tftp_ip>
execute certificate local import-pkcs12 {ftp | scp | sftp} <ip:port> <filename> <username>
     <password> <password> <name>
execute certificate local generate <certificate-name-string> <subject> <number> [<optional_
     information>]
execute certificate local list
```

Variable	Description
export <cert_name> <tftp_ip>	Export a certificate or request to a TFTP server. • `cert_name` - Name of the certificate. • `tftp_ip` - IP address of the TFTP server.
import <cert_name> <tftp_ip>	Import a signed certificate from a TFTP server.
import-pkcs12 {ftp | scp | sftp} <ip:port> <filename> <username> <password> <password> <name>	Import a certificate and private key from a PKCS#12 file. • `ftp`, `scp`, `sftp` - The type of server the file will be imported from. • `ip:port` - The server IP address and, optional, the port number. • `filename` - The path and file name on the server. • `username` - The user name on the server. • `password` - The user password. • `password` - The file password. • `name` - The certificate name.

generate <certificate-name_str> <number> <subject> [<optional_information>]	Generate a certificate request.
	• `certificate-name-string` - Enter a name for the certificate. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
	• `number` - The size, in bits, of the encryption key, `512`, `1024`, `1536`, or `2048`.
	• `subject` - Enter one of the following pieces of information to identify the FortiAnalyzer unit being certified:
	  • The FortiAnalyzer unit IP address
	  • The fully qualified domain name of the FortiAnalyzer unit
	  • An email address that identifies the FortiAnalyzer unit
	  • An IP address or domain name is preferable to an email address.
	• `optional_information` - Enter `optional_information` as required to further identify the unit. See Optional information variables on page 127 for more information.

list	Generate a list of CA certificates and requests that are on the FortiAnalyzer system.

Optional information variables

You must enter the optional variables in the order that they are listed in the table. To enter any optional variable you must enter all of the variables that come before it in the list.

For example, to enter the `organization_name_str`, you must first enter the `country_code_str`, `state_name_str`, and `city_name_str`.

While entering optional variables, you can type `?` for help on the next required variable.

Variable	Description
<country_code_str>	Enter the two-character country code.
<state_name_str>	Enter the name of the state or province where the FortiAnalyzer unit is located.

Variable	Description
<city_name_str>	Enter the name of the city, or town, where the person or organization certifying the FortiAnalyzer unit resides.
<organization-name_str>	Enter the name of the organization that is requesting the certificate for the FortiAnalyzer unit.
<organization-unit_name_str>	Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiAnalyzer unit.
<email_address_str>	Enter a contact email address for the FortiAnalyzer unit.

console

console baudrate

Use this command to get or set the console baudrate.

Syntax

```
execute console baudrate [9600 | 19200 | 38400 | 57600 | 115200]
```

If you do not specify a baudrate, the command returns the current baudrate.

Setting the baudrate will disconnect your console session.

Example

Get the baudrate:

```
execute console baudrate
```

The response is displayed:

```
current baud rate is: 9600
```

Set the baudrate to 19200:

```
execute console baudrate 19200
```

date

Get or set the FortiAnalyzer system date.

Syntax

```
execute date [<date_str>]
```

where

`date_str` has the form `mm/dd/yyyy`

- `mm` is the month and can be `1` to `12`
- `dd` is the day of the month and can be `1` to `31`
- `yyyy` is the year and can be `2001` to `2037`

If you do not specify a date, the command returns the current system date.

Dates entered will be validated - `mm` and `dd` require one or two digits, and `yyyy` requires four digits. Entering fewer digits will result in an error.

Example

This example sets the date to 29 September 2020:

```
execute date 9/29/2020
```

device

Use this command to change a device password or serial number when changing devices due to a hardware issue.

Syntax

```
execute device replace pw <device_name> <password>
execute device replace sn <device_name> <serial_number>
```

Variable	Description
pw	Replace the device password.
sn	Replace the device serial number.
<device_name>	The name of the device.
<password>	The new password for the new device.
<serial_number>	The new serial number for the new device, for example: `FWF40C391XXX0062`.

Example

```
execute device replace pw FGT600C2805030002
This operation will clear the password of the device.
Do you want to continue? (y/n)y
```

erase-disk

Overwrite the flash (boot device) with random data a specified number of times. When you run this command, you will be prompted to confirm the request.

Executing this command will overwrite all information on the FortiAnalyzer system's flash drive. The FortiAnalyzer system will no longer be able to boot up.

Syntax

```
execute erase-disk flash <erase-times>
```

Variable	Description
<erase-times>	Number of times to overwrite the flash with random data (1 - 35, default = 1).

factory-license

Use this command to enter a factory license key. This command is hidden.

Syntax

```
execute factory-license <key>
```

Variable	Description
<key>	The factory license key.

fmupdate

Import or export packages using the FTP, SCP, or FTFP servers, and import database files from a CD-ROM.

Syntax

```
execute fmupdate {ftp | scp | tftp} import <type> <remote_file> <ip> <port> <remote_path>
     <user> <password>
execute fmupdate {ftp | scp | tftp} export <type> <remote_file> <ip> <port> <remote_path>
     <user> <password>
```

Variables	Description
{ftp | scp | tftp}	Select the file transfer protocol to use: `ftp`, `scp`, or `tftp`.
<type>	Select the type of file to export or import. The following options are available: `av-ips`, `fct-av`, `url`, `spam`, `file-query`, `license-fgt`, `license-fct`, `custom-url`, or `domp`.
<remote_file>	Update manager packet file name on the server or host.
<ip>	Enter the FQDN or the IP address of the server.
<port>	Enter the port to connect to on the remote SCP host. Range: 1 to 65535
<remote_path>	Enter the name of the directory of the file to download from the FTP server or SCP host. If the directory name has spaces, use quotes instead.
<user>	Enter the user name to log into the FTP server or SCP host
<password>	Enter the password to log into the FTP server or SCP host

fmupdate cdrom

Import database files from a CD-ROM. The CD-ROM must be mounted first.

This command is only available on hardware-based FortiAnalyzer models that have CD-ROM drives.

Syntax

```
execute fmupdate cdrom import <type> <string>
execute fmupdate cdrom list <folder>
execute fmupdate cdrom mount
execute fmupdate cdrom unmount
```

Variables	Description
import	Import database files.
<type>	Set the packet type: `url`, `spam`, or `file-query`.
<string>	The FortiGuard packet file name on the CD TFTP driver.
list	List the packets in a specific folder.
<folder>	The name of the folder to list.
mount	Mount the CD-ROM.
unmount	Unmount the CD-ROM.

format

Format the hard disk on the FortiAnalyzer system. You can select to perform a secure (deep-erase) format which overwrites the hard disk with random data. You can also specify the number of time to erase the disks.

Syntax

```
execute format <disk | disk-ext3 | disk-ext4> <RAID level> deep-erase <erase-times>
```

When you run this command, you will be prompted to confirm the request.

Executing this command will erase all device settings/images, databases, and log data on the FortiAnalyzer system's hard drive. The FortiAnalyzer device's IP address, and routing information will be preserved.

Variable	Description
<disk | disk-ext3 | disk-ext4>	Select to format the hard disk or format the hard disk with ext3 or ext4 file system.
deep-erase	Overwrite the hard disk with random data. Selecting this option will take longer than a standard format.
<erase-times>	Number of times to overwrite the hard disk with random data. Range: 1 to 35. Default: `1`
<RAID level>	Enter the RAID level to be set on the device. This option is only available on FortiAnalyzer models that support RAID. Enter `*` to show available RAID levels.

iotop

Use this command to display system processes input/output usage information and to set the delay between iterations.

Syntax

```
execute iotop [delay]
```

Variable	Description
[delay]	The delay between iterations, in seconds (default = 2).

iotps

Use this command to list system processes sorted by their read/write system call rate.

Syntax

```
execute iotps <parameter> <parameter> <parameter> <parameter> <parameter> <parameter>
```

Variable	Description
<parameter>	Parameters: • -r • -w • -e • -t [intv]

log

Use the following commands to manage device logs:

log adom disk-quota	log dlp-files clear
log device disk-quota	log import
log device logstore	log ips-pkt clear
log device permissions	log quarantine-files clear
log device vdom	log storage-warning

log adom disk-quota

Set the ADOM disk quota.

Syntax

```
execute log adom disk-quota <adom_name> <value>
```

Variable	Description
<adom_name>	Enter the ADOM name, or enter All for all ADOMs.
<value>	Enter the disk quota value in megabytes.

log device disk-quota

Set the log device disk quota.

Syntax

```
execute log device disk-quota <device_id> <value>
```

Variable	Description
<device_id>	Enter the log device ID, or enter `All` for all devices.
<value>	Enter the disk quota value in megabytes.

log device logstore

Use this command to view and edit log storage information.

Syntax

```
execute log device logstore clear <device_id>
execute log device logstore list
```

Variable	Description
clear <device_id>	Remove leftover log directory.
list	List log storage directories.

log device permissions

Use this command to view and set log device permissions.

Syntax

```
execute log device permissions <device_id> <permission> {enable | disable}
```

Variable	Description
<device_id>	Enter the log device ID, or enter `All` for all devices. Example: `FWF40C3911000061`
<permission>	The following options are available: • `all`: All permissions • `logs`: Log permission • `content`: Content permission • `quar`: Quarantine permission • `ips`: IPS permission.
{enable | disable}	Enable/disable permissions.

log device vdom

Use this command to add, delete, or list VDOMs.

Syntax

```
execute log device vdom add <Device Name> <ADOM> <VDOM>
execute log device vdom delete <Device Name> <VDOM>
execute log device vdom delete-by-id <Device Name> <index>
execute log device vdom list <Device Name>
```

Variable	Description
add <Device Name> <ADOM> <VDOM>	Add a new VDOM to a device with the device name, the ADOM that contains the device, and the name of the new VDOM.
delete <Device Name> <VDOM>	Delete a VDOM from a device.
delete-by-id <Device Name> <index>	Delete a VDOM from a device by its index number.
list <Device Name>	List all the VDOMs on a device.

log dlp-files clear

Use this command to clear DLP log files on a specific log device.

Syntax

```
execute log dlp-files clear <device_name> <archive type>
```

Variable	Description
<device_name>	Enter the device name.
<archive type>	Enter the device archive type: `all`, `email`, `im`, `ftp`, `http`, or `mms`.

log import

Use this command to import log files from another device and replace the device ID on imported logs.

Syntax

```
execute log import <service> <ip:port> <user-name> <password> <file-name> <device-id>
```

Variable	Description
<service>	Enter the transfer protocol one of: `ftp`, `sftp`, `scp`,or `tftp`.

Variable	Description
<ip:port>	Server IP address or host name. Port is optional.
<user-name>	Enter the username.
<password>	Enter the password or '-' for no password. The `<password>` field is not required when `<service>` is `tftp`.
<file-name>	The file name (e.g. `dir/fgt.alog.log`) or directory name (e.g. `dir/subdir/`).
<device-id>	Replace the device ID on imported logs. Enter a device serial number of one of your log devices.

log ips-pkt clear

Use this command to clear IPS packet logs on a specific log device.

Syntax

```
execute log ips-pkt clear <device_name>
```

Variable	Description
<device_name>	Enter the device name.

log quarantine-files clear

Use this command to clear quarantine log files on a specific log device.

Syntax

```
execute log quarantine-files clear <device_name>
```

Variable	Description
<device_name>	Enter the device name.

log storage-warning

Reset the licensed VM storage size warning

Syntax

```
execute log storage-warning reset
```

log-aggregation

Immediately upload the log to the server.

Syntax

```
execute log-aggregation <id>
```

Variable	Description
<id>	The client ID, or `all` for all clients.

log-fetch

Use the following commands to fetch logs.

log-fetch client

Use these commands to manage client sessions.

Syntax

```
execute log-fetch client cancel <profile name>
execute log-fetch client list <profile name>
execute log-fetch client pause <profile name>
execute log-fetch client resume <profile name>
execute log-fetch client run <profile name>
execute log-fetch client view <profile name>
```

Variable	Description
cancel <profile name>	Cancel one session.
list <profile name>	List all sessions.
pause <profile name>	Pause one session.
resume <profile name>	Resume one session.
run <profile name>	Start a new session.
view <profile name>	View the session status.

log-fetch server

Use this command to manager the log fetching server.

Syntax

```
execute log-fetch server approve <session id>
execute log-fetch server cancel <session id>
execute log-fetch server deny <session id>
execute log-fetch server list
execute log-fetch server pause <session id>
execute log-fetch server resume <session id>
execute log-fetch server view <session id>
```

Variable	Description
approve <session id>	Approve a session.
cancel <session id>	Pause and clear one session or all sessions.
deny <session id>	Deny a session.
list	List all sessions.
pause <session id>	Pause a session.
resume <session id>	Resume a session.
view <session id>	View the session.

log-integrity

Query the log file's MD5 checksum and timestamp.

Syntax

```
execute log-integrity <device_name> <vdom name> <log_name>
```

Variable	Description
<device_name>	The name of the log device.
<vdom name>	The VDOM name.
<log_name>	The log file name.

lvm

With Logical Volume Manager (LVM), a FortiAnalyzer VM device can have up to twelve total log disks added to an instance. More space can be added by adding another disk and running the LVM extend command.

This command is only available on FortiAnalyzer VM models.

Syntax

```
execute lvm extend
execute lvm info
execute lvm start
```

Variable	Description
extend	Extend the LVM logical volume.
info	Get system LVM information.
start	Start using LVM.

migrate

Use this command to migrate all backup settings from the FTP, SCP, or SFTP server.

Syntax

```
execute migrate all-settings {ftp | scp | sftp} <ip:port> <string> <username> <password>
     <ssh-cert> [<crptpasswd>]
```

Variable	Description
{ftp | scp | sftp}	Enter the server type: `ftp`, `scp`, or `sftp`.
<ip:port>	Enter the server IP address and optionally, for FTP servers, the port number.
<string>	Enter the path and file name for the backup.
<username>	Enter username to use to log on the backup server.
<password>	Enter the password for the username on the backup server.
<ssh-cert>	Enter the SSH certification for the server. This option is only available for backup operations to SCP servers.
[<crptpasswd>]	Optional password to protect backup content. Use `any` for no password.

ping

Send an ICMP echo request (ping) to test the network connection between the FortiAnalyzer system and another network device.

Syntax

```
execute ping <ip | hostname>
```

Variable	Description
<ip | hostname>	IPv4 address or DNS resolvable hostname of network device to contact.

Example

This example shows how to ping a host with the IPv4 address `192.168.1.23`:

```
execute ping 192.168.1.23
```

ping6

Send an ICMP echo request (ping) to test the network connection between the FortiAnalyzer system and another network device.

Syntax

```
execute ping6 <ip | hostname>
```

Variable	Description
<ip | hostname>	Enter the IPv6 address or DNS resolvable hostname of network device to contact.

Example

This example shows how to ping a host with the IPv6 address 8001:0DB8:AC10:FE01:0:0:0:0:

```
execute ping6 8001:0DB8:AC10:FE01:0:0:0:0:
```

raid

This command allows you to add and delete RAID disks.

This command is only available on hardware-based FortiAnalyzer models that support RAID.

Syntax

```
execute raid add-disk <disk index>
execute raid delete-disk <disk index>
```

Variable	Description
add-disk <disk index>	Add a disk and give it an index number.
delete-disk <disk index>	Delete the specified disk.

reboot

Restart the FortiAnalyzer system. This command will disconnect all sessions on the FortiAnalyzer system.

Syntax

```
execute reboot
```

remove

Use this command to remove all custom settings in Logview, all reports for a specific device, and a security fabric from a specific ADOM.

Syntax

```
execute remove gui-logview-settings
execute remove reports [device-id]
execute remove security-facbric <adom-name> <security-fabric-name>
```

Variable	Description
<device-id>	The device identifier for the device that all reports are being removed from.
<adom-name>	The ADOM that contains the security fabric that is being removed.
<security-fabric-name>	The security fabric that is being removed.

Example

```
execute remove gui-logview-settings
This operation will Remove all custom settings in GUI LogView and reset to default for all
     users.
Do you want to continue? (y/n)y

Remove all custom settings in GUI LogView ...
Done! Reset all settings in GUI LogView to default.
```

reset

Use these commands to reset the FortiAnalyzer unit. These commands will disconnect all sessions and restart the FortiAnalyzerunit.

Syntax

```
execute reset adom-settings <adom> <version> <mr>
execute reset all-settings
execute reset all-except-ip
execute reset hitcount
```

Variable	Description
adom-settings <adom> <version> <mr>	Reset an ADOM's settings. • `<adom>`: The ADOM name. • `<version>`: The ADOM version. For example, `5` for 5.x releases. • `<mr>`: The major release number.
all-settings	Reset to factory default settings.
all-except-ip	Reset all settings except the current IP address and route information.
hitcount	Reset the dbcache and ADOM hitcounts.

restore

Use this command to:

- restore the configuration or database from a file
- change the FortiAnalyzer unit image
- Restore device logs, DLP archives, and reports from specified servers.

This command will disconnect all sessions and restart the FortiAnalyzer unit.

Syntax

```
execute restore all-settings {ftp | sftp} <ip:port> <filename> <username> <password>
     [<crptpasswd>] [option1+option2+...]
execute restore all-settings scp <ip> <filename> <username> <ssh-cert> [<crptpasswd>]
     [option1+option2+...]
execute restore image ftp <filepath> <ip:port> <username> <password>
execute restore image tftp <filename> <ip>
execute restore logs <device name(s)> {ftp | scp | sftp} <ip> <username> <password>
     <directory> [vdlist]
execute restore logs-only <device name(s)> {ftp | scp | sftp} <ip> <username> <password>
     <directory> [vdlist]
execute restore reports <report name(s)> {ftp | scp | sftp} <ip> <username> <password>
     <directory> [vdlist]
execute restore reports-config {<adom_name> | all]} {ftp | scp | sftp} <ip> <username>
     <password> <directory> [full]
```

Variable	Description
all-settings	Restore all FortiAnalyzersettings from a file on a FTP, SFTP, or SCP server. The new settings replace the existing settings, including administrator accounts and passwords.
image	Upload a firmware image from an FTP or TFTP server to the FortiAnalyzer unit. The FortiAnalyzer unit reboots, loading the new firmware.
logs	Restore device logs and DLP archives from a specified server.
logs-only	Restore device logs from a specified server.
reports	Restore reports from a specified server.
reports-config	Restore report configurations to a specified server.
ftp	Restore from an FTP server.
sftp	Restore from a SFTP server.
scp	Restore from an SCP server.
<ip:port>	Enter the IP address of the server to get the file from and optionally , for FTP servers, the port number.
<ip>	Enter the server IP address.
<device names>	Device name or names, separated by commas, or `all` for all devices. Example: `FWF40C3911000061`
<report name(s)>	Restore specific reports (separated by commas), `all` for all reports, or reports with names containing given pattern. A '`?`' matches any single character. A '`*`' matches any string, including the empty string, e.g.: • `foo`: for exact match • `*foo`: for report names ending with foo • `foo*`: for report names starting with foo • `*foo*`: for report names containing foo substring.

Variable	Description
{<adom_name> | all]}	Select to backup a specific ADOM or all ADOMs.
<filename>	Enter the file to get from the server. You can enter a path with the filename, if required.
<filepath>	Enter the file path on the FTP server.
<username>	The username to log on to the server. This option is not available for restore operations from TFTP servers.
<password>	Enter the password, or – if there is no password..
<ssh-cert>	Enter the SSH certificate used for user authentication on the SCP server.
[<crptpasswd>]	Optional password to protect backup content. Use `any` for no password.
[option1+option2+...]	Enter `keepbasic` to retain IP and routing information on the original unit.
<directory>	Enter the directory.
[full]	Reports configuration full restoration.

Example

This example shows how to upload a configuration file from a FTP server to the FortiAnalyzer unit. The name of the configuration file on the FTP server is `backupconfig`. The IP address of the FTP server is 192.168.1.23. The user is `admin` with a password of `mypasword`. The configuration file is located in the `/usr/local/backups/` directory on the FTP server.

```
execute restore all-settings ftp 192.168.1.23 /usr/local/backups/backupconfig admin
     mypasword
```

sensor

This command lists sensors and readings.

This command is only available on hardware-based FortiAnalyzer models.

Syntax

```
execute sensor detail
execute sensor list
```

Variable	Description
detail	List detailed sensors and readings.
list	List sensors and readings.

shutdown

Shut down the FortiAnalyzer system. This command will disconnect all sessions.

Syntax

```
execute shutdown
```

sql-local

Use this command to remove the SQL database and logs from the FortiAnalyzer system and to rebuild the database and devices.

When rebuilding the SQL database, new logs will not be available until the rebuild is complete. The time required to rebuild the database is dependent on the size of the database. Please plan a maintenance window to complete the database rebuild. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

The following features will not be available until after the SQL database rebuild has completed: FortiView, Log View, Event Management, and Reports.

Syntax

```
execute sql-local rebuild-adom <adom> ... <adom>
execute sql-local rebuild-db
execute sql-local rebuild-index <adom> <start-time > <end-time>
execute sql-local remove-db
```

Variable	Description
rebuild-adom	Rebuild log SQL database from log data for particular ADOMs.
rebuild-db	Rebuild entire log SQL database from log data. This operation will remove the SQL database and rebuild from log data. It will also reboot the device.
rebuild-index	Rebuild indexes for an ADOM.
remove-db	Remove the entire local SQL database.

Variable	Description
<adom>	The ADOM name. Multiple ADOM names can be entered when rebuilding ADOMs.
<start-time >	Enter the start time (timestamp or <yyyy-mm-dd hh:mm:ss>).
<end-time>	Enter the end time (timestamp or <yyyy-mm-dd hh:mm:ss>).
<log type>	Enter the log type from available log types, for example: `emailfilter`

sql-query-dataset

Use this command to execute a SQL dataset against the FortiAnalyzersystem.

Syntax

```
execute sql-query-dataset <adom> <dataset-name> <device/group name> <faz/dev> <start-time>
    <end-time>
```

Variable	Description
<adom_name>	Enter the ADOM name.
<dataset-name>	Enter the SQL dataset name.
<device/group name>	Enter the name of the device or device group.
<faz/dev>	Enter the reference time: FortiAnalyzer time or device time.
<start-time>	Enter the log start time (timestamp or <yyyy-mm-dd hh:mm:ss>).
<end-time>	Enter the log end time (timestamp or <yyyy-mm-dd hh:mm:ss>).

sql-query-generic

Use this command to execute a SQL statement against the FortiAnalyzer system.

Syntax

```
execute sql-query-generic <string>
```

Variable	Description
<string>	Specify the SQL statement to be executed.

sql-report

Use these commands to import and display language translation and font files, and run a SQL report schedule once against the FortiAnalyzer system.

Syntax

```
execute sql-report delete-font <font-name>
execute sql-report delete-lang <language-name>
execute sql-report delete-template adom-installed <adom> <language> [title]
execute sql-report delete-template device-default <dev-type> <language> [title]
execute sql-report export-lang <language-name> <service> <ip> <argument 1> <argument 2>
     <argument 3>
execute sql-report export-template adom-installed <adom> <service> <ip> <user> <password>
     <file name> [language] [title]
execute sql-report export-template device-default <dev-type> <service> <ip> <user>
     <password> <file name> [language] [title]
execute sql-report hcache-build <adom> <schedule-name> <start-time> <end-time>
execute sql-report hcache-check <adom> <schedule-name> <start-time> <end-time>
execute sql-report import-font <service> <ip> <argument 1> <argument 2> <argument 3>
execute sql-report import-lang <language-name> <service> <ip> <argument 1> <argument 2>
     <argument 3>
execute sql-report import-template <devtype> <service> <ip> <user> <password> <file name>
execute sql-report install-template <adom> <language> <service> <ip> <user> <password> <file
     name>
execute sql-report list <adom> [days-range] [layout-name]
execute sql-report list-fonts
execute sql-report list-lang [language]
execute sql-report list-schedule <adom> [sched-only | autocache-only | detail] [detail]
execute sql-report list-template adom-installed <adom> [language]
execute sql-report list-template device-default <dev-type> [language]
execute sql-report run <adom> <schedule-name> <start-time> <end-time>
execute sql-report view <data-type> <adom> <report-name>
```

Variable	Description
delete-font	Delete one font.
delete-lang	Delete one language translation file.
delete-template	Delete templates. • `adom-installed` - Delete report templates installed in ADOM. • `device-default` - Delete device type default report templates.
export-lang	Export a user-defined language translation file.
export-template	Export report templates. • `adom-installed` - Export ADOM report templates to file. • `device-default` - Export device type default report templates to file.
hcache-build	Build report hcache.
hcache-check	Check report hcache.

Variable	Description
import-font	Import one font.
import-lang	Import a user-defined language translation file.
import-template	Import per device type template from a configuration file.
install-template	Install specific language templates to an ADOM.
list	List recent generated reports.
list-fonts	List all imported fonts.
list-lang	Display all supported language translation files.
list-schedule	List report schedule and autocache information.
list-template	List templates. • `adom-installed` - Display report templates installed in ADOM. • `device-default` - Display device type default report templates.
run	Run a report once.
view	View report data.
<adom>	Specify the ADOM name.
<font-name>	The name of a font.
<dev-type>	Enter the device type abbreviation: • `FGT` - FortiGate • `FMG` - FortiManager • `FCT` - FortiClient • `FML` - FortiMail • `FWB` - FortiWeb • `FCH` - FortiCache • `FAZ` - FortiAnalyzer • `FSA` - FortiSandbox • `FDD` - FortiDDoS • `FAC` - FortiAuthenticator • `FPX` - FortiProxy
<language-name>	Enter the language name to import, export, or delete a language translation file, or select one of the following options: • `English` • `French` • `Japanese` • `Korean` • `Portuguese` • `Simplified_Chinese` • `Spanish` • `Traditional_Chinese`
<service>	Enter the transfer protocol: `ftp`, `sftp`, `scp`, or `tftp`. TFTP is not available for all commands.
<ip>	Enter the server IP address.
<argument 1>	For FTP, SFTP, or SCP, type a user name. For TFTP, enter a file name.
<argument 2>	For FTP, SFTP, or SCP, type a password or '-'. For TFTP, press `<enter>`.

Variable	Description
<argument 3>	Enter a file name and press <enter>.
<user>	Enter a user name for the remote server.
<password>	Enter the password, or –, for the remote server user.
<file name>	Enter the name of the file.
<data-type>	The data type to view. Must be `report-data`.
<report-name>	The name of the report to view.
<schedule-name>	Select one of the available report schedule names.
<start-time>	The start date and time of the report schedule, in the format: `"HH:MM yyyy/mm/dd"`
<end-time>	The enddate and time of the report schedule, in the format: `"HH:MM yyyy/mm/dd"`
[days-range]	The recent n days to list reports, from 1 to 99.
[layout-name]	One of the available SQL report layout names.
[language]	Enter the language abbreviation: • `en` - English • `de` - German • `es` - Spanish • `fr` - French • `it` - Italian • `ja` - Japanese • `ko` - Korean • `pt` - Portuguese • `ru` - Russian • `zh` - Simplified Chinese • `zh_Hant` - Traditional Chinese
[title]	Title of a specific report template.

ssh

Use this command to establish an SSH session with another system.

Syntax

```
execute ssh <destination> <username>
```

Variable	Description
<destination>	Enter the IP or FQ DNS resolvable hostname of the system you are connecting to.
<username>	Enter the user name to use to log on to the remote system.

To leave the SSH session type `exit`. To confirm that you are connected or disconnected from the SSH session, verify that the command prompt has changed.

ssh-known-hosts

Use this command to remove known SSH hosts.

Syntax

```
execute ssh-known-hosts remove-all
execute ssh-known-hosts remove-host <host/ip>
```

Variable	Description
remove-all	Remove all known SSH hosts.
remove-host	Remove the specified SSH hosts. • `<host/IP>` - The hostname or IP address of the SSH host to remove.

tac

Use this command to run a TAC report.

Syntax

```
execute tac report <file_name>
```

Variable	Description
<file_name>	Optional output file name.

time

Get or set the system time.

Syntax

```
execute time [<time_str>]
```

Variable	Description
[<time_str>]	The time of day, in the form `hh:mm:ss`. • `hh` is the hour and can be `00` to `23` • `mm` is the minutes and can be `00` to `59` • `ss` is the seconds and can be `00` to `59` All parts of the time are required. Single digits are allowed for each of `hh`, `mm`, and `ss`.

If you do not specify a time, the command returns the current system time.

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

top

Use this command to view the processes running on the FortiAnalyzer system.

Syntax

```
execute top <parameter> <parameter> ... <parameter>
```

Variable	Description
<parameter>	The following parameters can be used: `-hv | -bcHiOSs -d secs -n max -u|U user -p pid(s) -o field -w [cols]`

execute top help menu

Use the following commands when viewing the running processes. Press `h` or `?` for help.

Command	Description
Z,B,E,e	Global: 'Z' colors; 'B' bold; 'E'/'e' summary/task memory scale
l,t,m	Toggle Summary: 'l' load avg; 't' task/cpu stats; 'm' memory info
0,1,2,3,I	Toggle: '0' zeros; '1/2/3' cpus or numa node views; 'I' Irix mode
f,F,X	Fields: 'f'/'F' add/remove/order/sort; 'X' increase fixed-width
L,&,<,> .	Locate: 'L'/'&' find/again; Move sort column: '<'/'>' left/right
R,H,V,J .	Toggle: 'R' Sort; 'H' Threads; 'V' Forest view; 'J' Num justify

Command	Description
c,i,S,j .	Toggle: 'c' Cmd name/line; 'i' Idle; 'S' Time; 'j' Str justify
x,y.	Toggle highlights: 'x' sort field; 'y' running tasks
z,b.	Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y')
u,U,o,O .	Filter by: 'u'/'U' effective/any user; 'o'/'O' other criteria
n,#,^O.	Set: 'n'/'#' max tasks displayed; Show: Ctrl+'O' other filter(s)
C,....	Toggle scroll coordinates msg for: up,down,left,right,home,end
k,r	Manipulate tasks: 'k' kill; 'r' renice
d or s	Set update interval
W,Y	Write configuration file 'W'; Inspect other output 'Y'
q or <Esc>	Quit

traceroute

Test the connection between the FortiAnalyzer system and another network device, and display information about the network hops between the device and the FortiAnalyzer system.

Syntax

```
execute traceroute <host>
```

Variable	Description
<host>	Enter the IP address or hostname of network device.

traceroute6

Test the connection between the FortiAnalyzer system and another network device, and display information about the network hops between the device and the FortiAnalyzer system.

Syntax

```
execute traceroute6 <host>
```

Variable	Description
<host>	Enter the IPv6 address or hostname of network device.

diagnose

The `diagnose` commands display diagnostic information that help you to troubleshoot problems.

CLI commands and variables are case sensitive.

auto-delete	fortilogd	sniffer
cdb	fwmanager	sql
debug	ha	system
dlp-archives	hardware	test
dvm	log	upload
fmnetwork	pm2	vpn
fmupdate	report	

auto-delete

Use this command to view and configure auto-deletion settings.

Syntax

```
diagnose auto-delete dlp-files {delete-now | list}
diagnose auto-delete log-files {delete-now | list}
diagnose auto-delete quar-files {delete-now | list}
diagnose auto-delete report-files {delete-now | list}
```

Variable	Description
dlp-files {delete-now | list}	Delete or list DLP files. • `delete-now`: Delete DLP files right now according to system automatic deletion policy. • `list`: List DLP files according to system automatic deletion policy.
log-files {delete-now | list}	Delete or list log files. • `delete-now`: Delete log files right now according to system automatic deletion policy. • `list`: List log files according to system automatic deletion policy.
quar-files {delete-now | list}	Delete or list quarantine files.

Variable	Description
	• `delete-now`: Delete quarantine files right now according to system automatic deletion policy. • `list`: List quarantine files according to system automatic deletion policy.
report-files {delete-now | list}	Delete or list report files. • `delete-now`: Delete report files right now according to system automatic deletion policy. • `list`: List report files according to system automatic deletion policy.

cdb

Use this command to check the object configuration database integrity, the global policy assignment table, and repair configuration database.

Syntax

```
diagnose cdb check adom-revision [adom] [preview]
diagnose cdb check db-schema-version {get | reset | upgrade} [version]
diagnose cdb check update-devinfo <item> [new value] [0 | 1] [model-name]
diagnose cdb upgrade check <action>
diagnose cdb upgrade force-retry <action>
diagnose cdb upgrade log
diagnose cdb upgrade pending-list
diagnose cdb upgrade summary
```

Variable	Description
check adom-revision [adom] [preview]	Check or remove invalid ADOM revision database. Optionally, preview the check before running it.
check db-schema-version {get | reset | upgrade} [version]	Get, reset, or upgrade the database schema version.
check update-devinfo <item> [new value] [0 | 1] [model-name]	Update device information by directly changing the database. • `item`: Device information item • `new value`: Item new value. Default sump summary only. • `0 | 1`: update only empty values (default), or always update (1) • `model-name`: Only update on model name. Default: all models
upgrade check <action>	Perform a check to see if upgrade and repair is necessary. • `resync-dev-vdoms` - Resync and add any missing vdoms from device database to DVM database
upgrade force-retry <action>	Re-run an upgrade that was already performed in previous release.
upgrade log	Display the configuration database upgrade log.
upgrade pending-list	Display the list of upgrades scheduled for the next reboot.

Variable	Description
upgrade summary	Display the firmware upgrade summary.

debug

Use the following commands to debug the FortiAnalyzer.

debug application

Use these commands to view or set the debug levels for the FortiAnalyzer applications. All of the debug levels are 0 by default.

Syntax

```
diagnose debug application alertmail <integer>
diagnose debug application apiproxyd <integer>
diagnose debug application clusterd <integer>
diagnose debug application curl <integer>
diagnose debug application dmapi <integer>
diagnose debug application dns <integer>
diagnose debug application execmd <integer>
diagnose debug application fazcfgd <integer>
diagnose debug application fazmaild <integer>
diagnose debug application faznotify <integer>
diagnose debug application fazsvcd <integer>
diagnose debug application fazwatchd <integer>
diagnose debug application fdssvrd <integer>
diagnose debug application fgdsvr <integer>
diagnose debug application fgdupd <integer>
diagnose debug application fgfmsd <integer> [deviceName]
diagnose debug application filefwd <integer>
diagnose debug application fnbam <integer>
diagnose debug application fortilogd <integer>
diagnose debug application fortimanagerws <integer>
diagnose debug application fortimeter <integer>
diagnose debug application gui <integer>
diagnose debug application ha <integer>
diagnose debug application ipsec <integer>
diagnose debug application localmod <integer>
diagnose debug application log-aggregate <integer>
diagnose debug application logd <integer>
diagnose debug application log-fetchd <integer>
diagnose debug application logfiled <integer>
diagnose debug application logfwd <integer>
diagnose debug application lrm <integer>
diagnose debug application ntpd <integer>
diagnose debug application oftpd <integer> [<IP/deviceSerial/deviceName>]
```

```
diagnose debug application rptchkd <integer>
diagnose debug application scheduled <integer>
diagnose debug application snmpd <integer>
diagnose debug application sql_dashboard_rpt <integer>
diagnose debug application sql-integration <integer>
diagnose debug application sqllogd <integer>
diagnose debug application sqlplugind <integer>
diagnose debug application sqlrptcached <integer>
diagnose debug application ssh <integer>
diagnose debug application sshd <integer>
diagnose debug application storaged <integer>
diagnose debug application syncsched <integer>
diagnose debug application uploadd <integer>
diagnose debug application vmd <integer>
```

Variable	Description
alertmail <integer>	Set the debug level of the alert email daemon.
apiproxyd <integer>	Set the debug level of the API proxy daemon.
clusterd <integer>	Set the debug level of the clusterd daemon.
curl <integer>	This command is not in use.
dmapi <integer>	Set the debug level of the dmapi daemon.
dns <integer>	Set the debug level of DNS daemon.
execmd <integer>	Set the debug level of the execmd daemon.
fazcfgd <integer>	Set the debug level of the fazcfgd daemon.
fazmaild <integer>	Set the debug level of the fazmaild daemon.
faznotify <integer>	Set the debug level of the faznotify daemon.
fazsvcd <integer>	Set the debug level of the FAZ server daemon.
fazwatchd <integer>	Set the debug level of the fazwatchd daemon.
fdssvrd <integer>	Set the debug level of the FDS server daemon.
fgdsvr <integer>	Set the debug level of the FortiGuard query daemon.
fgdupd <integer>	Set the debug level of the FortiGuard update daemon.
fgfmsd <integer> [deviceName]	Set the debug level of FGFM daemon. Enter a device name to only show messages related to that device.
filefwd <integer>	Set the debug level of the filefwd daemon.
fnbam <integer>	Set the debug level of the Fortinet authentication module.
fortilogd <integer>	Set the debug level of the fortilogd daemon.
fortimanagerws <integer>	Set the debug level of the FortiAnalyzer Web Service.
fortimeter <integer>	Set the debug level of the FortiMeter daemon.
gui <integer>	Set the debug level of the GUI.

Variable	Description
ha <integer>	Set the debug level of HA.
ipsec <integer>	Set the debug level of the IPsec daemon.
localmod <integer>	Set the debug level of the localmod daemon.
log-aggregate <integer>	Set the debug level of the log aggregate daemon.
logd <integer>	Set the debug level of the log daemon.
log-fetchd <integer>	Set the debug level of the log fetcher daemon.
logfiled <integer>	Set the debug level of the logfilled daemon.
logfwd <integer>	Set the debug level of the logfwd daemon.
lrm <integer>	Set the debug level of the Log and Report Manager.
ntpd <integer>	Set the debug level of the Network Time Protocol (NTP) daemon.
oftpd <integer> [<IP/deviceSerial/deviceName>]	Set the debug level of the oftpd daemon. Enter an IPv4 address, device serial number, or device name to only show messages related to that device or IPv4 address.
rptchkd <integer>	Set the debug level of the rptchkd daemon.
scheduled <integer>	Set the debug level of the schedule task daemon.
snmpd <integer>	Set the debug level of the SNMP daemon.
sql_dashboard_rpt <integer>	Set the debug level of the SQL dashboard report daemon.
sql-integration <integer>	Set the debug level of SQL applications.
sqllogd <integer>	Set the debug level of SQL log daemon.
sqlplugind <integer>	Set the debug level of the SQL plugin daemon.
sqlrptcached <integer>	Set the debug level of the SQL report caching daemon.
ssh <integer>	Set the debug level of SSH protocol transactions.
sshd <integer>	Set the debug level of the SSH daemon.
storaged <integer>	Set the debug level of communication with java clients.
syncsched <integer>	Set the debug level of the syncsched daemon.
uploadd <integer>	Set the debug level of the upload daemon.
vmtools <integer>	Set the debug level for vmd.

Example

This example shows how to set the debug level to 7 for the upload daemon:

```
diagnose debug application uploadd 7
```

debug backup-oldformat-script-logs

Use this command to backup script log files that failed to be upgraded to the FTP server.

Syntax

```
diagnose debug backup-oldformat-script-logs <ip> <string> <username> <password>
```

Variable	Description
<ip>	Enter the FTP server IP address.
<string>	Enter the path/filename to save the log to the FTP server.
<username>	Enter the user name on the FTP server.
<password>	Enter the password associated with the user name.

debug cli

Use this command to set the debug level of CLI.

Syntax

```
diagnose debug cli <integer>
```

Variable	Description
<integer>	Set the debug level of the CLI (0 - 8, default = 3).

debug console

Use this command to enable or disable console debugging.

Syntax

```
diagnose debug console {enable | disable}
```

Variable	Description
{enable | disable}	Enable/disable console debugging.

debug crashlog

Use this command to clear the debug crash log.

Syntax

```
diagnose debug crashlog clear
diagnose debug crashlog read
```

Variable	Description
clear	Clear the crash log.
read	Read the crash log.

debug disable

Use this command to disable debugging.

Syntax

```
diagnose debug disable
```

debug enable

Use this command to enable debugging.

Syntax

```
diagnose debug enable
```

debug info

Use this command to show active debug level settings.

Syntax

```
diagnose debug info
```

debug klog

Use this command to show all kernel logs.

Syntax

```
diagnose debug klog
```

debug reset

Use this command reset the debug level settings. All debug settings will be reset.

Syntax

```
diagnose debug reset
```

debug service

Use this command to view or set the debug level of various service daemons.

Syntax

```
diagnose debug service cdb <integer>
diagnose debug service cmdb <integer>
diagnose debug service csf <integer>
diagnose debug service dvmcmd <integer>
diagnose debug service dvmdb <integer>
diagnose debug service fazconf <integer>
diagnose debug service main <integer>
daignose debug service sys <integer>
diagnose debug service task <integer>
```

Variable	Description
<integer>	The debug level

debug sysinfo

Use this command to show system information.

Syntax

```
diagnose debug sysinfo
```

debug sysinfo-log

Use this command to generate one system info log file every two minutes.

Syntax

```
diagnose debug sysinfo-log {on | off}
```

debug sysinfo-log-backup

Use this command to backup all sysinfo log files to an FTP server.

Syntax

```
diagnose debug sysinfo-log-backup <server> <filepath> <user> <password>
```

Variable	Description
<server>	Enter the FTP server IP address.
<filepath>	Enter the path/filename to save the log to the FTP server.
<user>	Enter the user name on the FTP server.
<password>	Enter the password associated with the user name.

debug sysinfo-log-list

Use this command to display system information elogs.

Syntax

```
diagnose debug sysinfo-log-list <integer>
```

Variable	Description
<integer>	Display the last n elogs (default = 10).

debug timestamp

Use this command to enable or disable debug timestamp.

Syntax

```
diagnose debug timestamp {enable | disable}
```

debug vminfo

Use this command to show VM license information.

This command is only available on FortiAnalyzer VM models.

Syntax

```
diagnose debug vminfo
```

dlp-archives

Use this command to manage the DLP archives.

Syntax

```
diagnose dlp-archives quar-cache list-all-process
diagnose dlp-archives quar-cache kill-process <pid>
diagnose dlp-archives rebuild-quar-db
diagnose dlp-archives remove
diagnose dlp-archives statistics {show | flush}
diagnose dlp-archives status
diagnose dlp-archives upgrade
```

Variable	Description
quar-cache list-all-process	List all processes that are using the quarantine cache.
quar-cache kill-process <pid>	Kill a process that is using the quarantine cache.
rebuild-quar-db	Rebuild Quarantine Cache DB
remove	Remove all upgrading DLP archives.
statistics {show | flush}	Display or flush the quarantined and DLP archived file statistics.
status	Running status.
upgrade	Upgrade the DLP archives.

dvm

Use the following commands for DVM related settings.

dvm adom

Use this command to list ADOMs.

Syntax

```
diagnose dvm adom list
diagnose dvm adom unlock <adom>
```

Variable	Description
list	List ADOMs, state, product, OS version (OSVER), major release (MR), name, mode, VPN management, and IPS.
unlock <adom>	Remove DVM lock by FortiManager.

dvm capability

Use this command to set the DVM capability.

Syntax

```
diagnose dvm capability set {all | standard}
diagnose dvm capability show
```

Variable	Description
set {all | standard}	Set the capability to all or standard.
show	Show what the capability is set to.

dvm chassis

Use this command to list chassis and supported chassis models.

Syntax

```
diagnose dvm chassis list
diagnose dvm chassis supported models
```

Variable	Description
list	List chassis.
supported-models	List supported chassis models.

dvm check-integrity

Use this command to check the DVM database integrity.

Syntax

```
diagnose dvm check-integrity
```

dvm csf

Use this command to print the CSF configuration.

Syntax

```
diagnose dvm csf <adom> <category>
```

Variable	Description
<adom>	The ADOM name.
<category>	The category: • `all`: Dump all CSF categories • `group`: Dump CSF group • `intf-role`: Dump interface role • `user-device`: Dump user device

dvm debug

Use this command to enable or disable debug channels.

Syntax

```
diagnose dvm debug {enable | disable} <channel> <channel> <channel> ... <channel>
```

Variable	Description
{enable | disable}	Enable/disable debug channels.
<channel>	The following channels are available: `all`, `dvm_db`, `dvm_dev`, `shelfmgr`, `ipmi`, `lib`, `dvmcmd`, `dvmcore`, `gui`, and `monitor`.

dvm device

Use this command to list devices or objects referencing a device.

Syntax

```
diagnose dvm device delete <adom> <device>
diagnose dvm device dynobj <device>
diagnose dvm device list <device> <vdom>
diagnose dvm device monitor <device> <api>
diagnose dvm device object-reference <device> <vdom> <category> <object>
```

Variable	Description
delete <adom> <device>	Delete a device in a specific ADOM.
dynobj <device>	List dynamic objects on this device.
list <device> <vdom>	List devices. Optionally, enter a device or VDOM name.
monitor <device> <api>	JSON API for device monitor. Specify the device name and the monitor API name.
object-reference <device> <vdom> <category> <object>	List object reference. Specify the device name, VDOM, category (or *all* for all categories), and object.

dvm device-tree-update

Use this command to enable or disable device tree automatic updates.

Syntax

```
diagnose dvm device-tree-update {enable | disable}
```

Variable	Description
{enable | disable}	Enable/disable device tree automatic updates.

dvm extender

Use these commands to list FortiExtender devices and synchronize FortiExtender data via JSON.

Syntax

```
diagnose dvm extender list [devname]
diagnose dvm extender sync-extender-data <devname> [savedb] [syncadom] [task]
```

Variable	Description
list [device]	List FortiExtender devices, or those connected to a specific device.
sync-extender-data <devname> [savedb] [syncadom] [task]	Synchronize FortiExtender data by JSON. Optionally: save the data to the database, synchronize the ADOM, and/or create a task.

dvm fap

Use this command to list the FortiAP devices connected to a device.

Syntax

```
diagnose dvm fap list <devname>
```

Variable	Description
<devname>	The name of the device.

dvm fsw

Use this command to list the FortiSwitch devices connected to a device.

Syntax

```
diagnose dvm fsw list <devname>
```

Variable	Description
<devname>	The name of the device.

dvm group

Use this command to list groups.

Syntax

```
diagnose dvm group list
```

Variable	Description
list	List groups.

dvm lock

Use this command to print the DVM lock states.

Syntax

```
diagnose dvm lock
```

dvm proc

Use this command to list DVM process (dvmcmd) information.

Syntax

```
diagnose dvm proc list
```

dvm remove

Use this command to remove all unused IPS package files.

Syntax

```
diagnose dvm remove unused-ips-packages
```

dvm supported-platforms

Use this command to list supported platforms.

Syntax

```
diagnose dvm supported-platforms list <detail>
diagnose dvm supported-platforms mr-list
diagnose dvm supported-platforms fortiswitch
```

Variable	Description
list <detail>	List supported platforms by device type. Enter *detail* to show details with syntax support.
mr-list	List supported platforms by major release.
fortiswitch	List supported platforms in FortiSwitch manager.

dvm task

Use this command to repair or reset the task database.

Syntax

```
diagnose dvm task list <adom> <type>
diagnose dvm task repair
diagnose dvm task reset
```

Variable	Description
list <adom> <type>	List task database information.

Variable	Description
repair	Repair the task database while preserving existing data where possible. The FortiAnalyzer will reboot after the repairs.
reset	Reset the task database to its factory default state. All existing tasks and the task history will be erased. The FortiAnalyzer will reboot after the reset.

dvm transaction-flag

Use this command to edit or display DVM transaction flags.

Syntax

```
diagnose dvm transaction-flag [abort | debug | none]
```

Variable	Description
transaction-flag [abort | debug | none]	Set the transaction flag.

dvm workflow

Use this command to edit or display workflow information.

Syntax

```
diagnose dvm workflow log-list <adom_name> <workflow_session_ID>
diagnose dvm workflow session-list [<adom_name>]
```

Variable	Description
log list <adom_name> <workflow_session_ID>	List workflow session logs.
session list [<adom_name>]	List workflow sessions.

fmnetwork

Use the following commands for network related settings.

fmnetwork arp

Use this command to manage ARP.

Syntax

```
diagnose fmnetwork arp del <intf-name> <ip>
diagnose fmnetwork arp list
```

Variable	Description
del <intf-name> <ip>	Delete an ARP entry.
list	List ARP entries.

fmnetwork interface

Use this command to view interface information.

Syntax

```
diagnose fmnetwork interface detail <portX>
diagnose fmnetwork interface list <portx>
```

Variable	Description
detail <portX>	View a specific interface's details, for example: `port1`.
list <portX>	List all interface details.

fmnetwork netstat

Use this command to view network statistics.

Syntax

```
diagnose fmnetwork netstat list [-r]
diagnose fmnetwork netstat tcp [-r]
diagnose fmnetwork netstat udp [-r]
```

Variable	Description
list [-r]	List all connections, or use -r to list only resolved IP addresses.
tcp [-r]	List all TCP connections, or use -r to list only resolved IP addresses.
udp [-r]	List all UDP connections, or use -r to list only resolved IP addresses.

fmupdate

Use these commands to diagnose update services.

Syntax

```
diagnose fmupdate dbcontract [fds | fgd] [serial_num]
diagnose fmupdate del-device {fct | fds | fgd | fgc} <serial_num> <UID>
diagnose fmupdate del-log
diagnose fmupdate del-object {fds | fct | fgd | fgc | fgd-fgfq} [object_type] [object_
     version]
diagnose fmupdate del-serverlist {fct | fds | fgd | fgc}
diagnose fmupdate fct-getobject
diagnose fmupdate fds-dump-breg
diagnose fmupdate fds-dump-fmgi
diagnose fmupdate fds-dump-srul
diagnose fmupdate fds-get-downstream-device [serial_num]
diagnose fmupdate fds-getobject
diagnose fmupdate fds-update-info
diagnose fmupdate fgd-asdevice-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d} {all | <serial>}
     <integer>
diagnose fmupdate fgd-asserver-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d}
diagnose fmupdate fgd-bandwidth {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate fgd-dbver {wf | as | av-query}
diagnose fmupdate fgd-del-db {wf | as | av-query | file-query}
diagnose fmupdate fgd-get-downstream-device
diagnose fmupdate fgd-test-client <ip> <serial> <string> <integer>
diagnose fmupdate fgd-url-rating <ip> <serial> <version> <url>
diagnose fmupdate fgd-wfas-clear-log
diagnose fmupdate fgd-wfas-log {name | ip} <string>
diagnose fmupdate fgd-wfas-rate {wf | av | as_ip | as_url | as_hash}
diagnose fmupdate fgd-wfdevice-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d} {all | <serial>}
     {periods}
diagnose fmupdate fgd-wfserver-stat {top10sites | top10devices} {10m | 30m | 1h | 6h | 12h |
     24h | 7d}
diagnose fmupdate fgt-del-statistics
diagnose fmupdate fgt-del-um-db
diagnose fmupdate fmg-statistic-info
diagnose fmupdate fortitoken {seriallist | add | del} {add | del | required}
diagnose fmupdate get-device {fct | fds | fgd | fgc} <serial_num>
diagnose fmupdate list-object {fds | fct | fgd | fgc | fgd-fgfq} [type] [version]
diagnose fmupdate service-restart {fct | fds | fgd | fgc}
diagnose fmupdate show-bandwidth {fct | fgt | fml | faz} {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate show-dev-obj <string>
diagnose fmupdate updatenow {fds | fgd | fct}
diagnose fmupdate update-status {fds | fct | fgd | fgc}
diagnose fmupdate view-configure {fds | fct | fgd | fgc}
diagnose fmupdate view-linkd-log {fds | fct | fgd | fgc}
diagnose fmupdate view-serverlist {fds | fct | fgd | fgc}
diagnose fmupdate view-service-info {fds | fgd}
diagnose fmupdate vm-license
```

Variables	Description
dbcontract [fds | fgd] [serial_num]	Dumb the subscriber contract.
del-device {fct | fds | fgd | fgc} <serial_num> <UID>	Delete a device. UID is required for FortiClient (fct) only.

Variables	Description
del-log	Delete all the logs for FDS and FortiGuard update events.
del-object {fds | fct | fgd | fgc | fgd-fgfq} [object_type] [object_ version]	Remove all objects from the specified service. Optionally, enter the object type and version or time.
del-serverlist {fct | fds | fgd | fgc}	Delete the server list file (fdni.dat) from the specified service.
fct-getobject	Get the versions of all FortiClient objects.
fds-dump-breg	Dump the FDS beta serial numbers.
fds-dump-fmgi	Dump FMGI (Object description details) file
fds-dump-srul	Dump the FDS select filtering rules.
fds-get-downstream-device [serial_num]	Get information of all downstream FortiGate antivirus-IPS devices. Optionally, enter the device serial number.
fds-getobject	Get the versions of all FortiGate objects.
fds-update-info	Display scheduled update information.
fgd-asdevice-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d} {all | <serial>} <integer>	Display antispam device statistics for single or all devices. • <integer>: Number of time periods to display (optional, default = 1).
fgd-asserver-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d}	Display antispam server statistics.
fgd-bandwidth {1h | 6h | 12h | 24h | 7d | 30d}	Display the download bandwidth.
fgd-dbver {wf | as | av-query}	Get the version of the database. Optionally, enter the database type.
fgd-del-db {wf | as | av-query | file-query}	Delete FortiGuard database. Optionally, enter the database type.
fgd-get-downstream-device	Get information on all downstream FortiGate web filter and spam devices.
fgd-test-client <ip> <serial> <string> <integer>	Execute FortiGuard test client. Optionally, enter the hostname or IPv4 address of the FGD server, the serial number of the device, and the query number per second or URL.
fgd-url-rating <ip> <serial> <version> <url>	Rate URLs within the FortiManager database using the FortiGate serial number. Optionally, enter the category version and URL.
fgd-wfas-clear-log	Clear the FortiGuard service log file.
fgd-wfas-log {name | ip} <string>	View the FortiGuard service log file. Optionally, enter the device filter type, and device name or IPv4 address.
fgd-wfas-rate {wf | av | as_ip | as_ url | as_hash}	Get the web filter / antispam rating speed. Optionally, enter the server type.

Variables	Description
fgd-wfdevice-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d} <serialnum>	Display web filter device statistics. Optionally, enter a specific device's serial number.
fgd-wfserver-stat {top10sites | top10devices} {10m | 30m | 1h | 6h | 12h | 24h | 7d}	Display web filter server statistics for the top 10 sites or devices. Optionally, enter the time frame to cover.
fgt-del-statistics	Remove all statistics (antivirus / IPS and web filter / antispam). This command requires a reboot.
fgt-del-um-db	Remove UM and UM-GUI databases. This command requires a reboot. **Note**: um.db is a sqlite3 database that update manager uses internally. It will store AV/IPS package information of downloaded packages. This command removes the database file information. The package is not removed. After the reboot, the database will be recreated. Use this command if you suspect the database file is corrupted.
fmg-statistic-info	Display statistic information for FortiManager and Java Client.
fortitoken {seriallist | add | del} {add | del | required}	FortiToken related operations.
get-device {fct | fds | fgd | fgc} <serial_num>	Get device information. Optionally, enter a serial number.
list-object {fds | fct | fgd | fgc | fgd-fgfq} [type] [version]	List downloaded objects of linkd service. Optional enter the object type and version or time.
service-restart {fct | fds | fgd | fgc}	Restart the linkd service.
show-bandwidth {fct | fgt | fml | faz} {1h | 6h | 12h | 24h | 7d | 30d}	Display the download bandwidth for a device type over a specified time period.
show-dev-obj [serial_num]	Display an objects version of a device. Optionally, enter a serial number.
updatenow {fds | fgd | fct}	Update immediately.
update-status {fds | fct | fgd | fgc}	Display the update status.
view-configure {fds | fct | fgd | fgc}	Dump the running configuration.
view-linkd-log {fds | fct | fgd | fgc}	View the linkd log file.
view-serverlist {fds | fct | fgd | fgc}	Dump the server list.
view-service-info {fds | fgd}	Display the service information.
vm-license	Dump the FortiGate VM license.

fortilogd

Use this command to view FortiLog daemon information.

Syntax

```
diagnose fortilogd lograte
diagnose fortilogd msgrate
diagnose fortilogd msgrate-device
diagnose fortilogd msgrate-total
diagnose fortilogd msgrate-type
diagnose fortilogd msgstat [flush]
diagnose fortilogd status
```

Variable	Description
lograte	Display the log rate.
msgrate	Display log message rate.
msgrate-device	Display log message rate devices.
msgrate-total	Display log message rate totals.
msgrate-type	Display log message rate types.
msgstat [flush]	Display or flush log message statuses.
status	Running status.

fwmanager

Use the following commands for fwmanager related settings.

Syntaxcancel

```
diagnose fwmanager cancel-devsched <dev_name> <firmware_version> <release_type> <build_num>
     <date_time>
diagnose fwmanager cancel-grpsched <group_name> <firmware_version> <release_type> <build_
     num> <date_time>
diagnose fwmanager delete-all
diagnose fwmanager delete-imported-images
diagnose fwmanager delete-official-images
diagnose fwmanager delete-serverlist
diagnose fwmanager fwm-log
diagnose fwmanager getall-schedule
diagnose fwmanager getdev-schedule <string>
diagnose fwmanager getgrp-schedule <string>
diagnose fwmanager imported-imagelist
diagnose fwmanager official-imagelist <platform>
diagnose fwmanager reset-schedule-database
diagnose fwmanager serverlist [raw]
diagnose fwmanager service-restart
diagnose fwmanager set-devsched <string> <firmware_version> <release_type> <build_num>
     <date_num>
diagnose fwmanager set-grpsched <string> <firmware_version> <release_type> <build_num>
     <date_num>
```

Variable	Description
cancel-devsched <dev_name> <firmware_version> <release_ type> <build_num> <date_time>	Cancel an upgrade schedule for a device. For special branches, the release type is the branch point. The build number for official releases is always `-1`, for special releases it is the build number. The date and time format is: `YYYY/MM/DD_hh:mm:ss`
cancel-grpsched <group_name> <firmware_version> <release_ type> <build_num> <date_time>	Cancel an upgrade schedule for a group. For special branches, the release type is the branch point. The build number for official releases is always `-1`, for special releases it is the build number. The date and time format is: `YYYY/MM/DD_hh:mm:ss`
delete-all	Remove everything in the firmware manager folder. This command requires a reboot.
delete-imported-images	Remove all imported images. This command requires a reboot.
delete-official-images	Remove all official images. This command requires a reboot.
delete-serverlist	Remove the server list file (fdni.dat). This command requires a reboot.
fwm-log	View the firmware manager log file.
getall-schedule	Display all upgrade schedules recorded.
getdev-schedule <dev_name>	Get scheduled upgrades for the device.
getgrp-schedule <group_name>	Get scheduled upgrades for this group.
imported-imagelist	Get the imported firmware image list
official-imagelist <platform>	Get the official firmware image list for the platform.
reset-schedule-database	Cleanup and initialize the schedule database and restart the server.
serverlist [raw]	Dump the server list, optionally in raw format.
service-restart	Restart the firmware manager server.
set-devsched <dev_name> <firmware_version> <release_ type> <build_num> <date_num>	Create an upgrade schedule for a device.
set-grpsched <group_name> <firmware_version> <release_ type> <build_num> <date_num>	Create an upgrade schedule for a group.

ha

Use this command to view and manage high availability.

Syntax

```
diagnose ha debug-sync {on | off}
```

```
diagnose ha dump-datalog
diagnose ha failover <device-id>
diagnose ha force-cfg-resync
diagnose ha load-balance
diagnose ha restart-init-sync
diagnose ha stats [verbose]
diagnose ha status
```

Variable	Description
debug-sync {on | off}	Turn synchronized data debug on or off.
dump-datalog	Dump the HA data log.
failover <device-id>	Force HA failover. Use the device ID of the new primary device , or re-elect from backup FortiAnalyzer devices if not specified.
force-resync	Force HA to re-synchronization the configuration.
load-balanace	HA load balance status
restart-init-sync	Restart HA initial sync. This command can only be run on the primary unit.
stats [verbose]	Get HA statistics. Optionally, get verbose output.
status	Get HA status.

hardware

Use this command to view hardware information. This command provides comprehensive system information including: CPU, memory, disk, and RAID information.

Syntax

```
diagnose hardware info
```

log

Use the following command to view device log usage.

Syntax

```
diagnose log device [<device-id> | adom] [adom-name | all | *]
```

Variable	Description
[<device-id> | adom]	Optionally filter by device ID or ADOM.
[adom-name | all | *]	Optionalyl filter by ADOM name when filtering by ADOM.

pm2

Use these commands to check the integrity of the database.

Syntax

```
diagnose pm2 check-integrity {all adom device global ips task ncmdb}
diagnose pm2 print <log-type>
```

Variable	Description
check-integrity {all adom device global ips task ncmdb}	Check the integrity of the database. Multiple database categories can be selected.
print <log-type>	Print the database log messages.

report

Use this command to check the SQL database.

Syntax

```
diagnose report clean {ldap-cache | report-queue}
diagnose report status [pending | running]
```

Variable	Description
clean {ldap-cache | report-queue}	Cleanup the SQL report queue or LDAP cache.
status [pending | running]	Check status information on pending and running reports.

sniffer

Use this command to perform a packet trace on one or more network interfaces.

Packet capture, also known as sniffing, records some or all of the packets seen by a network interface. By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiAnalyzer units have a built-in sniffer. Packet capture on FortiAnalyzer units is similar to that of FortiGate units. Packet capture is displayed on the CLI, which you may be able to save to a file for later analysis, depending on your CLI client.

Packet capture output is printed to your CLI display until you stop it by pressing `CTRL + C`, or until it reaches the number of packets that you have specified to capture.

Packet capture can be very resource intensive. To minimize the performance impact on your FortiAnalyzer unit, use packet capture only during periods of minimal traffic, with a serial console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

Syntax

```
diagnose sniffer packet <interface> <filter> <verbose> <count> <Timestamp format>
```

Variable	Description
<interface>	Type the name of a network interface whose packets you want to capture, such as `port1`, or type `any` to capture packets on all network interfaces.

<filter>	Type either `none` to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as `'tcp port 25'`. Surround the filter string in quotes.
	The filter uses the following syntax:
	`'[[src|dst] host {<host1_fqdn> | <host1_ipv4>}] [and|or]`
	`[[src|dst] host {<host2_fqdn> | <host2_ipv4>}] [and|or]`
	`[[arp|ip|gre|esp|udp|tcp] port <port1_int>] [and|or]`
	`[[arp|ip|gre|esp|udp|tcp] port <port2_int>]'`
	To display only the traffic between two hosts, specify the IP addresses of both hosts. To display only forward or only reply packets, indicate which host is the source and which is the destination.
	For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter:
	`'udp and port 1812 and src host 1.example.com and dst \`
	`( 2.example.com or 2.example.com \)'`

<verbose>	Type one of the following numbers indicating the depth of packet headers and payloads to capture: • `1`: print header of packets (default) • `2`: print header and data from ip of packets • `3`: print header and data from ethernet of packets (if available) For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (`3`).
<count>	Type the number of packets to capture before stopping.

Variable	Description
	If you do not specify a number, the command will continue to capture packets until you press `CTRL + C`.
<Timestamp format>	Type the timestamp format. • `a`: absolute UTC time, yyyy-mm-dd hh:mm:ss.ms • `l`: absolute LOCAL time, yyyy-mm-dd hh:mm:ss.ms • `otherwise`: relative to the start of sniffing, ss.ms

Example 1

The following example captures the first three packets' worth of traffic, of any port number or protocol and between any source and destination (a filter of `none`), that passes through the network interface named port1. The capture uses a low level of verbosity (indicated by `1`).

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiAnalyzer# diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.918957 192.168.0.1.36701 -> 192.168.0.2.22: ack 2598697710
0.919024 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697710 ack 2587945850
0.919061 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697826 ack 2587945850
```

If you are familiar with the TCP protocol, you may notice that the packets are from the middle of a TCP connection. Because port 22 is used (highlighted above in bold), which is the standard port number for SSH, the packets might be from an SSH session.

Example 2

The following example captures packets traffic on TCP port 80 (typically HTTP) between two hosts, 192.168.0.1 and 192.168.0.2. The capture uses a low level of verbosity (indicated by `1`). Because the filter does not specify either host as the source or destination in the IP header (`src` or `dst`), the sniffer captures both forward and reply traffic.

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses CTRL + C. The sniffer then confirms that five packets were seen by that network interface.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiAnalyzer# diag sniffer packet port1 'host 192.168.0.2 or host 192.168.0.1 and tcp port
     80' 1
192.168.0.2.3625 -> 192.168.0.1.80: syn 2057246590
192.168.0.1.80 -> 192.168.0.2.3625: syn 3291168205 ack 2057246591
192.168.0.2.3625 -> 192.168.0.1.80: ack 3291168206
192.168.0.2.3625 -> 192.168.0.1.80: psh 2057246591 ack 3291168206
192.168.0.1.80 -> 192.168.0.2.3625: ack 2057247265
5 packets received by filter
0 packets dropped by kernel
```

Example 3

The following example captures all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP address. The capture uses a high level of verbosity (indicated by `3`).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses CTRL + C. The sniffer then confirms that five packets were seen by that network interface.

Verbose output can be very long. As a result, output shown below is truncated after only one packet.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiAnalyzer # diag sniffer port1 'tcp port 443' 3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000 0009 0f09 0001 0009 0f89 2914 0800 4500 ..........)...E.
0x0010 003c 73d1 4000 4006 3bc6 d157 fede ac16 .<s.@.@.;..W....
0x0020 0ed8 c442 01bb 2d66 d8d2 0000 0000 a002 ...B..-f........
0x0030 16d0 4f72 0000 0204 05b4 0402 080a 03ab ..Or............
0x0040 86bb 0000 0000 0103 0303 ..........
```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encodings other than US-ASCII. It is usually preferable to analyze the output by loading it into in a network protocol analyzer application such as Wireshark (http://www.wireshark.org/).

For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output. Methods may vary. See the documentation for your CLI client.

Requirements

- terminal emulation software such as PuTTY
- a plain text editor such as Notepad
- a Perl interpreter
- network protocol analyzer software such as Wireshark

To view packet capture output using PuTTY and Wireshark:

1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the Fortinet appliance using either a local serial console, SSH, or Telnet connection.
3. Type the packet capture command, such as:
   ```
   diagnose sniffer packet port1 'tcp port 541' 3 100
   ```
   but do not press `Enter` yet.
4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select *Change Settings*.
   A dialog appears where you can configure PuTTY to save output to a plain text file.
5. In the *Category* tree on the left, go to *Session* > *Logging*.
6. In *Session logging*, select *Printable output*.
7. In *Log file name*, click the *Browse* button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file. (You do not need to save it with the `.log` file extension.)

8. Click *Apply*.
9. Press Enter to send the CLI command to the FortiMail unit, beginning packet capture.
10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press `CTRL + C` to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad++.
13. Delete the first and last lines, which look something like this:
    ```
    =~=~=~=~=~=~=~=~=~=~=~=~= PuTTY log 2018.09.29 08:03:40 =~=~=~=~=~=~=~=~=~=~=~=~=
    Fortinet-2000 #
    ```
    These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.
14. Convert the plain text file to a format recognizable by your network protocol analyzer application.
    You can convert the plain text file to a format (.pcap) recognizable by Wireshark using the fgt2eth.pl Perl script. To download fgt2eth.pl, see the Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer.

    

    The fgt2eth.pl script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

    To use fgt2eth.pl, open a command prompt, then enter a command such as the following:
    ```
    fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
    ```
    where:
    - `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
    - `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
    - `packet_capture.pcap` is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved
15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.
    For additional information on packet capture, see the Fortinet Knowledge Base article Using the FortiOS built-in packet sniffer.

sql

Use this command to diagnose the SQL database.

Syntax

```
diagnose sql config auto-cache-delay [set <seconds>| reset]
diagnose sql config debug-filter [set | test] [string]
diagnose sql config deferred-index-timespan [set <value>]
diagnose sql config hcache-agg-step [reset | set <integer>]
diagnose sql config hcache-base-trim-interval [reset | set <integer>]
diagnose sql config hcache-max-fv-row [reset | set <integer>]
diagnose sql config hcache-max-rpt-row [reset | set <integer>]
diagnose sql config report-engine [set gen2]
```

```
diagnose sql config topdev-log-thres [reset | set <integer>]
diagnose sql config topdev-num-max [reset | set <integer>]
diagnose sql hcache add-task <adom> <norm-query-hash> <agg-level> <timestamp> <num-of-days>
diagnose sql hcache aggregate debug {on | off}
diagnose sql hcache aggregate debug-file {show | delete | upload <ftp host> <ftp dir> <ftp
     user name> <ftp password>}
diagnose sql hcache aggregate status <adom> <query-hash/tag> <detail>
diagnose sql hcache dump-task <filter>
diagnose sql hcache list <adom> <start-time> <end-time> <query-tag/norm-qry-hash/sql> <is-
     fortiview> <max-time-scale>
diagnose sql hcache rebuild-both <start-time> <end-time>
diagnose sql hcache rebuild-fortiview <start-time> <end-time>
diagnose sql hcache rebuild-report <start-time> <end-time>
diagnose sql hcache rebuild-status
diagnose sql hcache show hcache <adom> <id>
diagnose sql hcache show time <time> <time> <time> <time>
diagnose sql hcache status {all | <adom>}
diagnose sql process kill <pid>
diagnose sql process list [full]
diagnose sql remove {hcache <adom> [fast] | query-cache | rebuild-db-flag | tmp-table}
diagnose sql show {db-size | hcache-size | log-filters | log-stfile <device-id> <vdom> |
     policy-info <adom>}
diagnose sql status {rebuild-adom <adom> | rebuild-db | run_sql_rpt | sqlplugind |
     sqlreportd}
diagnose sql upload <ftp_host_ip> <ftp_directory> <ftp_user_name> <ftp_password>
```

Variable	Description
config auto-cache-delay [set <seconds>| reset]	Show, set, or reset the auto-cache delay, in seconds (default = 300).
config debug-filter {set | test} <string>	Set or test the SQL plugin debug filter.
config deferred-index-timespan [set <value>]	View or set the time span for the deferred index (default = 10000).
config hcache-agg-step [reset | set <integer>]	Show, set, or reset the hcache aggregation step (default = 10).
config hcache-base-trim-interval [reset | set <integer>]	Show, set, or reset the hcache base trim interval (default = 172800).
config hcache-max-fv-row [reset | set <integer>]	Show, set, or reset max row number for fortiview hcache (default = 100000).
config hcache-max-rpt-row [reset | set <integer>]	Show, set, or reset max row number for report hcache (default = 18000).
config report-engine [set gen2]	Show or set the report-engine version.
config topdev-log-thres [reset | set <integer>]	Show, set, or reset log threshold of top devices.
config topdev-num-max [reset | set <integer>]	Show, set, or reset max number of top devices.

Variable	Description
hcache add-task <adom> <norm-query-hash> <agg-level> <timestamp> <num-of-days>	Add an hcache task: • `adom`: The ADOM name. • `norm-query-hash`: The normalized query hash. • `agg-level`: The aggregation level. • `timestamp`: The timestamp (format = yyyy-mm-dd hh:mm:ss). • `num-of-days`: The number of days (1, 3, or 30).
hcache aggregate debug {on | off}	Turn debug on or off.
hcache aggregate debug-file {show | delete | upload <ftp host> <ftp dir> <ftp user name> <ftp password>}	Delete, show, or upload the debug file. The following input is required when uploading the debug file: • `ftp host`: The FTP host IP address. • `ftp dir`: The FTP directory. • `ftp user name`: The FTP user name. • `ftp password`: The FTP password.
hcache aggregate status <adom> <query-hash/tag> <detail>	Show hcache aggregation info: • `adom`: The ADOM name, or `all` for all ADOMs. • `query-hash/tag`: The hash or tag filter query, or `all` for all queries. • `detail`: Show detailed information.
hcache dump-task <filter>	Dump hcache tasks. Enter the task filter.
hcache list <adom> <start-time> <end-time> <query-tag/norm-qry-hash/sql> <is-fortiview> <max-time-scale>	List hcaches: • `adom`: The ADOM name. • `start-time`: The start time (format: yyyy-mm-dd hh:mm:ss). • `end-time`: The end time (format: yyyy-mm-dd hh:mm:ss). • `query-tag/norm-qry-hash/sql`: The query tag, normalized query hash, or sql statement. • `is-fortiview`: Enter `1` for FortiView, or `0` for report. • `max-time-scale`: Maximum timescale.
hcache rebuild-both <start-time> <end-time>	Rebuild hcache for both report and FortiView. Start and end times are in the format yyyy-mm-dd hh:mm:ss.
hcache rebuild-fortiview <start-time> <end-time>	Rebuild hcache for FortiView only. Start and end times are in the format yyyy-mm-dd hh:mm:ss.
hcache rebuild-report <start-time> <end-time>	Rebuild hcache for report only. Start and end times are in the format yyyy-mm-dd hh:mm:ss.
hcache rebuild-status	Show report hcache rebuild/check status.
hcache show hcache <adom> <id>	Show hcache information. Enter the ADOM name and hcache ID.
hcache show time <time> <time> <time> <time>	Show hcache time. Enter up to four timestamps.
hcache status {all | <adom>}	Show detailed hcache information per ADOM or for all ADOMs.

Variable	Description
process kill <pid>	Kill a running query.
process list [full]	List running query processes.
remove {hcache <adom> [fast] | query-cache | rebuild-db-flag | tmp-table}	Remove the selected information: • `hcache`: Remove the hcache tables created for the SQL report. Enter `fast` to not remove the hcache result tables. • `query-cache`: Remove the SQL query cache for log search. • `rebuild-db-flag`: Remove the rebuild database flag. The system will exit the rebuild database state. • `tmp-table`: Remove the SQL database temporary tables.
show {db-size | hcache-size | log-filters | log-stfile <device-id> <vdom> | policy-info <adom>}	Show the database, hcache size, log filters, or log status file: • `db-size`: Show database size. • `hcache-size`: Show hcache size. • `log-filters`: Show log view searching filters. • `log-stfile`: Show logstatus file for the specified device (for HA cluster, input the member's serial number) and VDOM. • `policy-info`: Show policy uuid and name map.
status {rebuild-adom <adom> | rebuild-db | run_sql_rpt | sqlplugind | sqlreportd}	Show the status: • `rebuild-adom <adom>`: Show SQL log database rebuild status of ADOMs. • `rebuild-db`: Show SQL log database rebuild status. • `run-sql-rpt`: Show run_sql_rpt status. • `sqlplugind`: Show sqlplugind status. • `sqlreportd`: Show sqlreportd status.
upload <ftp_host_ip> <ftp_ directory> <ftp_user_name> <ftp_password>	Upload sqlplugind messages / pgsvr logs via FTP.

system

Use the following commands for system related settings.

system admin-session

Use this command to view and kill log in sessions.

Syntax

```
diagnose system admin-session kill <sid>
diagnose system admin-session list
diagnose system admin-session status
```

Variable	Description
kill <sid>	Kill a current session. • <sid>: Session ID
list	List log in sessions.
status	Show the current session.

system disk

Use this command to view disk diagnostic information.

This command is only available on hardware-based FortiAnalyzer models.

Syntax

```
diagnose system disk attributes
diagnose system disk disable
diagnose system disk enable
diagnose system disk health
diagnose system disk info
diagnose system disk errors
```

Variable	Description
attributes	Show vendor specific SMART attributes.
disable	Disable SMART support.
enable	Enable SMART support.
health	Show the SMART health status.
info	Show the SMART information.
errors	Show the SMART error logs.

system export

Use this command to export logs.

Syntax

```
diagnose system export crashlog <ftp server> <user> <password> <directory> <filename>
diagnose system export fmwslog {sftp | ftp} <type> <(s)ftp server> <username> <password>
     <directory> <filename>
diagnose system export raidlog <ftp server> <username> <password> <directory> <filename>
```

```
diagnose system export umlog {sftp | ftp} <type> <(s)ftp server> <username> <password>
     <directory> <filename>
diagnose system export upgradelog <ftp server> <username> <password> <directory> <filename>
```

Variable	Description
crashlog <ftp server> <user> <password> <directory> <filename>	Export the crash log.
fmwslog {sftp | ftp} <type> < (s)ftp server> <username> <password> <directory> <filename>	Export the web service log files. The type is the log file prefix and can be: `SENT`, `RECV`, or `TEST`.
raidlog <ftp server> <username> <password> <directory> <filename>	Export the RAID log. This command is only available on devices that support RAID.
umlog {sftp | ftp} <type> < (s)ftp server> <username> <password> <directory> <filename>	Export the update manager and firmware manager log files.
upgradelog <ftp server> <username> <password> <directory> <filename>	Export the upgrade error log.

system flash

Use this command to diagnose the flash memory.

Syntax

```
diagnose system flash list
```

Variable	Description
list	List flash images. The information displayed includes the image name, version, total size (KB), used (KB), percent used, boot image, and running image.

system fsck

Use this command to check and repair the file system, and to reset the disk mount count.

Syntax

```
diagnose system fsck harddisk
diagnose system fsck reset-mount-count
```

Variable	Description
harddisk	Check and repair the file system, then reboot the system.
reset-mount-count	Reset the mount-count of the disk on the next reboot.

system geoip

Use these commands to get geoip information.

FortiAnalyzer uses a MaxMind GeoLite database of mappings between geographic regions and all public IPv4 addresses that are known to originate from them.

Syntax

```
diagnose system geoip dump
diagnose system geoip info
diagnose system geoip ip <ip>
```

Variable	Description
dump	Display all geographic IP information.
info	Display a brief geography IP information.
ip <ip>	Find the specified IP address' country.

Example

Find the country of the IP address 4.3.2.1:

```
FAZVM64 # diagnose system geoip ip 4.3.2.1
4.3.2.1 : US - United States
```

system geoip-city

Use these commands to get geographic IP information at a city level.

Syntax

```
diagnose system geoip-city info
diagnose system geoip-city ip <ip version> <ip>
```

Variable	Description
info	Display geographic IP information.
ip <ip version> <ip>	Find the specified IP address' city.

system ntp

Use this command to list NTP server information.

Syntax

```
diagnose system ntp status
```

Variable	Description
status	List NTP server information.

system print

Use this command to print server information.

Syntax

```
diagnose system print certificate
diagnose system print cpuinfo
diagnose system print df
diagnose system print hosts
diagnose system print interface <interface>
diagnose system print loadavg
diagnose system print netstat
diagnose system print partitions
diagnose system print route
diagnose system print rtcache
diagnose system print slabinfo
diagnose system print sockets
diagnose system print uptime
```

Variable	Description
certificate	Print the IPsec certificate.
cpuinfo	Print the CPU information.
df	Print the file system disk space usage.
hosts	Print the static table lookup for host names.
interface <interface>	Print the specified interface's information.
loadavg	Print the average load of the system.
netstat	Print the network statistics for active Internet connections (servers and established).
partitions	Print the disk partition information.
route	Print the main route list.

Variable	Description
rtcache	Print the contents of the routing cache.
slabinfo	Print the slab allocator statistics.
sockets	Print the currently used socket ports.
uptime	Print how long the system has been running.

system process

Use this command to view and kill processes.

Syntax

```
diagnose system process kill -<signal> <pid>
diagnose system process killall {Scriptmgr | deploymgr | fgfm}
diagnose system process list
```

Variable	Description
kill -<signal> <pid>	Kill a process: • -<signal>: Signal name or number, such as -9 or -KILL • <pid>: Process ID
killall {Scriptmgr | deploymgr | fgfm}	Kill all the related processes.
list	List all processes running on the FortiAnalyzer. The information displayed includes the PID, user, VSZ, stat, and command.

system raid

Use this command to view RAID information.

This command is only available on hardware-based FortiAnalyzer models that support RAID.

Syntax

```
diagnose system raid hwinfo
diagnose system raid status
```

Variable	Description
hwinfo	Show RAID controller hardware information.

Variable	Description
status	Show RAID status.

system route

Use this command to help diagnose routes. The listed information includes the destination IP, gateway IP, netmask, flags, metric, reference, use, and interface for each IPv4 route.

Syntax

```
diagnose system route list
```

system route6

Use this command to help diagnose routes. The listed information includes the destination IP, gateway IP, netmask, flags, metric, reference, use, and interface for each IPv6 route.

Syntax

```
diagnose system route6 list
```

system server

Use this command to start the FortiAnalyzer server.

Syntax

```
diagnose system server start
```

test

Use the following commands to test the FortiAnalyzer.

test application

Use this command to test application daemons. Enter an unassigned integer value to see the available options for each command.

Syntax

```
diagnose test application apiproxyd <integer> <integer> ... <integer>
diagnose test application clusterd <integer> <integer> ... <integer>
diagnose test application execmd <integer> <integer> ... <integer>
diagnose test application fazcfgd <integer> <integer> ... <integer>
diagnose test application fazmaild <integer> <integer> ... <integer>
diagnose test application faznotify <integer> <integer> ... <integer>
diagnose test application fazsvcd <integer> <integer> ... <integer>
diagnose test application fazwatchd <integer> <integer> ... <integer>
diagnose test application filefwd <integer> <integer> ... <integer>
diagnose test application fortilogd <integer> <integer> ... <integer>
diagnose test application logfiled <integer> <integer> ... <integer>
diagnose test application logfwd <integer> <integer> ... <integer>
diagnose test application log-fetchd <integer> <integer> ... <integer>
diagnose test application miglogd <integer> <integer> ... <integer>
diagnose test application oftpd <integer> <integer> ... <integer>
diagnose test application rptchkd <integer> <integer> ... <integer>
diagnose test application snmpd <integer> <integer> ... <integer>
diagnose test application sqllogd <integer> <integer> ... <integer>
diagnose test application sqlrptcached <integer> <integer> ... <integer>
diagnose test application syncsched <integer> <integer> ... <integer>
diagnose test application uploadd <integer> <integer> ... <integer>
```

Variable	Description
apiproxyd <integer> ...	API proxy daemon test usage: • 1: show PID • 2: show statistics and state • 20: fsa tracer log request • 21: fsa tracer log request • 99: restart daemon
clusterd <integer> ...	Clusterd daemon test usage: • 0: Usage • 1: Thread pool status • 2: Log Cluster core • 3: Devices cache module • 4: Logging Topology module • 5: Avatar uploading module • 6: Meta-CSF uploading module • 7: Meta-InterfaceRole module • 8: Tunnel module • 9: oftpd file fwd module • 10: Service module • 97: HA module • 98: Monitor status • 99: Restart clusterd • 100: Restart clusterd and clusterd-monitor
execmd <integer> ...	Execmd daemon test usage: • 1: show PID

Variable	Description
	• 2: show statistics and state • 3: reset statistics and state • 99: restart daemon
fazcfgd <integer> ...	Fazcfg daemon test usage: • 1: show PID • 2: show statistics • 40: DVM cache diag info • 41: CSF diag info • 42: IntfRole diag info • 48: test update link prefixes file • 49: test update webfilter categories description file • 50: test get app icon • 51: test update app logo files • 52: dvm call stats • 53: dvm call stats clear • 54: check ips/app meta-data update • 55: log disk readahead get • 56: log disk readahead toggle • 57: fix redis service • 58: check redis service • 60: test fortigate restful api • 82: list avatar meta-data • 83: rebuild avatar meta-data table • 84: rebuild ips meta-data table • 85: rebuild app meta-data table • 86: rebuild FortiClient Vulnerability meta-data table • 88: update ffdb meta-data • 90: use built-in TIDB package and disable updating it • 91: enable updating TIDB package • 92: disable updating TIDB package • 99: restart daemon
fazmaild <integer> ...	Fazmaild daemon test usage: • 1: show PID and daemon status • 2: show runtime status • 90: pause sending mail • 91: resume sending mail • 99: restart fazmaild daemon
faznotify <integer> ...	Faznotify daemon test usage: • 0: usage information • 1: show faznotify pid • 2: show faznotify statistics [clear]

Variable	Description
	• 10: send a faznotify <adom> <id> <send-data> • 20: show active channel • 29: delete active channel <adom> <id> • 30: pause active channel <seconds> • 99: restart
fazsvcd <integer> ...	Fazsvcd daemon test usage: • 1: show PID • 2: show daemon stats and status • 3: list async search threads • 4: dump async search slot info • 5: show cache builder stats • 6: dump cache builder playlist • 7: dump log search filters • 10: show database log stats aggregated per day • 11: show received log stats aggregated per day • 50: enable or disable cache builder • 51: enable or disable auto custom index • 52: enable or disable skip-index usage • 60: rawlog idx cache test • 61: logbrowse cache stats • 70: show stats for device vdom cache • 71: show stats for remote fortiview and reports • 75: data masking test: <passwd> <plaint test> <1|0 (high secure)> [do_ unmasking] • 99: restart daemon
fazwatchd <integer> ...	Fazwatchd daemon test usage: • 1: show summary • 99: restart daemon
filefwd <integer> ...	Filefwd daemon test usage: • 1: show daemon PID • 2: show daemon stats • 3: show threads stats • 99: restart daemon
fortilogd <integer> ...	Fortilogd Diag test usage: • 0: usage information • 1: show fortilogd PID • 2: dump message status • 3: logstat status • 4: client devices status • 5: print log received • 6: switch on/off debug messages • 7: log forwarding prep status

Variable	Description
	• 8: show logUID info • 9: device log cache reloading status • 10: dz_client cache status • 11: file stats • 12: stop/restart receiving logs • 99: restart fortilogd
logfiled <integer> ...	Logfile daemon test usage: • 1: show PID • 2: show statistics and state • 4: show ADOM statistics • 5: show device statistics • 6: show auto-del statistics • 7: show log file disk usage • 8: update log file disk usage • 90: reset statistics and state • 91: force to preen content files info • 99: restart daemon
logfwd <integer> ...	Logfwd daemon test usage: • 0: Usage • 1: Dump log-forward configurations • 2: Dump thread-pool status • 3: Dump log-forwarding status • 98: Reset log-forwarding stats • 99: Restart logfwd
log-fetchd <integer> ...	Log-fetch daemon test usage: • 1: show PID • 2: show states • 3: show running sessions • 99: restart the daemon
miglogd <integer> ...	Miglogd daemon test usage: • 1: show PID • 2: dump memory pool • 99: restart daemon
oftpd <integer> ...	Oftpd daemon test usage: • 1: show PID • 2: show statistics and state • 3: show connected device name and IP • 4: show detailed session state • 5: show oftp request statistics • 6: show cmdb device cache • 7: show logfwd thread stats • 8: show tasklist statistics

Variable	Description
	• 9: show unreg dev cache • 10: log cluster bridge stats • 12: show HA group cache • 13: show file fwd stats • 22: dump oftp-restapi-sched status • 30: dump csf groups data in all adoms in json string • 32: reschedule all restapi task for designated devid • 50: display logtypes for all devid • 90: reload un-reg device tree • 91: delete designated csf group • 92: reload reg dev cache • 99: restart daemon
rptchkd <integer> ...	Sqlrptcache daemon test usage: • 1: show PID • 2: show statistics and state • 3: reset statistics and state • 4: list adoms • 5: re-check an adom • 99: restart daemon
snmpd <integer> ...	SNMP daemon test usage: • 1: display daemon pid • 2: display snmp statistics • 3: clear snmp statistics • 4: generate test trap (cpu high) • 5: generate test traps (log alert, rate, data rate) • 6: generate test traps (licensed gb/day, device quota) • 99: restart daemon
sqllogd <integer> ...	SqlLog daemon test usage: • 1: show PID • 2: show statistics and state • 3: show worker init state • 4: show worker thread info • 5: show log device scan info, optionally filter by <devid> • 7: show ADOM device list by <adom-name> • 8: show logUID info • 9: show ADOM scan sync info, optionally filter by <adom> • 10: show FortiClient dev to sql-ID (sID) map • 11: show devtable cache info • 12: show intfrole cache info • 41: show worker 1 info • 51: show worker 1 registered log devices • 61: show worker 1 open log file cache • 70: show sql database building progress

Variable	Description
	• 71: show the progress of upgrading log files into per-vdom storage • 72: run the upgrading log files into per-vdom storage • 80: show daemon status flags • 81: show debug zone devices status • 82: show all adoms with member devices or filer by <adom-name> • 83: show all registered logdevs • 84: show all unreg logdevs • 95: request to rebuild SQL database for local event logs • 96: resend all pending batch files to sqlplugind • 97: rebuilding warm restart • 98: set worker assignment to policy 'round-robin' or 'adom-affinity', daemon will restart on policy change. • 99: restart daemon • 200: diag for log based alert (event mgmt) .. • 201: diag for utmref cache .. • 202: diag for fgt-fct corelation .. • 203: diag for logstat .. • 204: diag for IoC .. • 205: diag for endpoint and enduser .. • 206: diag for ueba .. • 207: diag for FSA scan session .. • 208: diag for audit report event process .. • 221: estimated browsing time stats • 222: fsa devmap cache info • 224: fgt lograte cache info • 225: dump enum field error cache • 226: reset enum field error cache
sqlrptcached <integer> ...	Sqlrptcache daemon test usage: • 1: show PID • 2: show statistics and state • 3: reset statistics and state • 99: restart daemon
syncsched <integer> ...	syncsched daemon test usage: • 1: show daemon PID • 2: show report nodes states • 3: show report syncing state • 4: show ha sync peers • 10: sync reports with peer • 11: fsync stat • 12: fsync reload • 99: restart daemon
uploadd <integer> ...	Uploadd daemon test usage: • 1: show PID

Variable	Description
	• 2: show statistics and state • 3: reset statistics and state • 4: show uploadd queues content • 5: show upload server state • 50: clear log queue [mirror server1] • 51: clear log queue [mirror server2] • 52: clear log queue [mirror server3] • 53: clear log queue [backup] • 54: clear log queue [original request] • 55: clear log queues [all] • 56: clear report queue • 99: restart daemon

test connection

Test the connection to the mail server and syslog server.

Syntax

```
diagnose test connection fortianalyzer <ip>
diagnose test connection mailserver <server-name> <mail-from> <mail-to>
diagnose test connection syslogserver <server-name>
```

Variable	Description
fortianalyzer <ip>	Test the connection to the FortiAnalyzer.
mailserver <server-name> <mail-from> <mail-to>	Test the connection to the mail server.
syslogserver <server-name>	Test the connection to the syslog server.

test policy-check

Check policy consistency.

Syntax

```
diagnose test policy-check flush
diagnose test policy-check list
```

Variable	Description
flush	Flush all policy check sessions.
list	List all policy check sessions.

test search

Test the search daemon.

Syntax

```
diagnose test search flush
diagnose test search list
```

Variable	Description
flush	Flush all search sessions.
list	List all search sessions.

test sftp

Use this command to test the secure file transfer protocol (SFTP) scheduled backup.

Syntax

```
diagnose test sftp auth <sftp server> <username> <password> <directory>
```

Variable	Description
<sftp server>	SFTP server IP address.
<username>	SFTP server username.
<password>	SFTP server password.
<directory>	The directory on the SFTP server where you want to put the file (default = /).

upload

Use the following commands for upload related settings.

upload clear

Use this command to clear the upload request.

Syntax

```
diagnose upload clear log {all | backup | mirror 1 | mirror 2 | mirror 3 | original}
diagnose upload clear report
```

Variable	Description
log {all | original | backup | mirror 1 | mirror 2 | mirror 3	Clear log uploading requests. • `all`: Clear all log uploading requests. • `backup`: Clear log uploading requests in the backup queue. • `mirror 1`: Clear log uploading requests in the mirror queue for server 1. • `mirror 2`: Clear log uploading requests in the mirror queue for server 2. • `mirror 3`: Clear log uploading requests in the mirror queue for server 3. • `original`: Clear log uploading requests in the original queue.
report	Clear all report upload requests.

upload status

Use this command to get the running status on files in the upload queue.

Syntax

```
diagnose upload status
```

vpn

Use this command to flush SAD entries and list tunnel information.

Syntax

```
diagnose vpn tunnel flush-SAD
diagnose vpn tunnel list
```

Variable	Description
flush-SAD	Flush the SAD entries.
list	List tunnel information.

get

The `get` commands display a part of your FortiAnalyzer unit's configuration in the form of a list of settings and their values.

Although not explicitly shown in this section, for all `config` commands there are related get and show commands that display that part of the configuration. `get` and `show` commands use the same syntax as their related `config` command, unless otherwise specified.

CLI commands and variables are case sensitive.

The get command displays all settings, including settings that are in their default state.

Unlike the `show` command, `get` requires that the object or table whose settings you want to display are specified, unless the command is being used from within an object or table.

For example, at the root prompt, this command would be valid:

```
get system status
```

and this command would not:

```
get
```

fmupdate analyzer	system admin	system global	system ntp
fmupdate av-ips	system alert-console	system ha	system password-policy
fmupdate disk-quota	system alertemail	system interface	system performance
fmupdate fct-services	system alert-event	system locallog	system report
fmupdate fds-setting	system auto-delete	system log	system route
fmupdate multilayer	system backup	system log-fetch	system route6
fmupdate publicnetwork	system central-management	system log-forward	system snmp
fmupdate server-access-priorities	system certificate	system log-forward-service	system sql
fmupdate server-override-status	system dns	system loglimits	system status
fmupdate service	system fips	system mail	system syslog
fmupdate web-spam	system fortiview	system metadata	system workflow

fmupdate analyzer

Use this command to view the virus report to FDS.

Syntax

```
get fmupdate analyzer virusreport
```

fmupdate av-ips

Use these commands to view AV/IPS update settings.

Syntax

```
get fmupdate av-ips advanced-log
get fmupdate av-ips web-proxy
```

Example

This example shows the output for `get fmupdate av-ips web-proxy`:

```
ip : 0.0.0.0
ip6 : ::
mode : proxy
password : *
port : 80
status : disable
username : (null)
```

fmupdate custom-url-list

Use this command to view the custom URL database.

Syntax

```
get fmupdate custom-url-list
```

fmupdate disk-quota

Use this command to view the disk quota for the update manager.

Syntax

```
get fmupdate disk-quota
```

Example

This example shows the output for `get fmupdate disk-quota`:

```
value : 51200
```

fmupdate fct-services

Use this command to view FortiClient update services configuration.

Syntax

```
get fmupdate fct-services
```

Example

This example shows the output for `get fmupdate fct-services`:

```
status : enable
port : 80
```

fmupdate fds-setting

Use this command to view FDS parameters.

Syntax

```
get fmupdate fds-setting
```

Example

This example shows the output for `get fmupdate fds-setting`:

```
User-Agent : Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
fds-pull-interval : 240
fds-ssl-protocol : tlsv1.2
fmtr-log : info
linkd-log : info
max-av-ips-version : 20
max-work : 1
push-override:
```

```
push-override-to-client:
send_report : disable
send_setup : disable
server-override:
system-support-faz : 5.0 5.2 5.4 5.6 6.0
system-support-fct :
system-support-fgt :
system-support-fml :
system-support-fsa :
system-support-fsw :
umsvc-log : info
unreg-dev-option : add-service
```

fmupdate multilayer

Use this command to view multilayer mode configuration.

Syntax

```
get fmupdate multilayer
```

fmupdate publicnetwork

Use this command to view public network configuration.

Syntax

```
get fmupdate publicnetwork
```

fmupdate server-access-priorities

Use this command to view server access priorities.

Syntax

```
get fmupdate server-access-priorities
```

Example

This example shows the output for `get fmupdate server-access-priorities`:

```
access-public : disable
av-ips : disable
```

```
private-server:
web-spam : enable
```

fmupdate server-override-status

Use this command to view server override status configuration.

Syntax

```
get fmupdate server-override-status
```

fmupdate service

Use this command to view update manager service configuration.

Syntax

```
get fmupdate service
```

Example

This example shows the output for `get fmupdate service`:

```
avips : enable
query-geoip : enable
```

fmupdate web-spam

Use these commands to view web spam configuration.

Syntax

```
get fmupdate web-spam fgd-setting
get fmupdate web-spam web-proxy
```

Example

This example shows the output for `get fmupdate web-spam web-proxy`:

```
ip : 0.0.0.0
ip6 : ::
mode : proxy
```

```
password : *
port : 80
status : disable
username : (null)
```

system admin

Use these commands to view admin configuration.

Syntax

```
get system admin group [group name]
get system admin ldap [server entry name]
get system admin profile [profile ID]
get system admin radius [server entry name]
get system admin setting
get system admin tacacs [server entry name]
get system admin user [username]
```

Example

This example shows the output for `get system admin setting`:

```
access-banner : disable
admin-https-redirect: enable
admin-login-max : 256
admin_server_cert : server.crt
banner-message : (null)
gui-theme : blue
http_port : 80
https_port : 443
idle_timeout : 480
objects-force-deletion: enable
shell-access : disable
show-add-multiple : disable
show-checkbox-in-table: disable
show-device-import-export: disable
show-hostname : disable
show-log-forwarding : enable
unreg_dev_opt : add_allow_service
webadmin_language : auto_detect
```

system alert-console

Use this command to view the alert console settings.

Syntax

```
get system alert-console
```

Example

This example shows the output for `get system alert-console`:

```
period : 7
severity-level : emergency
```

system alertemail

Use this command to view alert email settings.

Syntax

```
get system alertemail
```

Example

This example shows the output for `get system alertemail`:

```
authentication : enable
fromaddress : (null)
fromname : (null)
smtppassword : *
smtpport : 25
smtpserver : (null)
smtpuser : (null)
```

system alert-event

Use this command to view alert event information.

Syntax

```
get system alert-event [alert name]
```

Example

This example shows the output for an alert event named `Test` that has default values:

```
name : Test
alert-destination:
```

```
enable-generic-text : disable
enable-severity-filter: disable
event-time-period : 0.5
generic-text : (null)
num-events : 1
severity-filter : high
severity-level-comp : =
severity-level-logs : no-check
```

system auto-delete

Use this command to view automatic deletion policies for logs, reports, DLP files, and quarantined files.

Syntax

```
get system auto-delete
```

system backup

Use the following commands to view backups:

Syntax

```
get system backup all-settings
get system backup status
```

Example

This example shows the output for `get system backup status`:

```
All-Settings Backup
   Last Backup: Tue Sep 29 08:03:35 2020
   Next Backup: N/A
```

system central-management

Use this command to view the central management configuration.

Syntax

```
get system central-management
```

Example

This example shows the output for `get system central-management`:

```
type : fortimanager
allow-monitor : enable
fmg : (null)
enc-algorithm : default
authorized-manager-only: enable
serial-number :
```

system certificate

Use these commands to view certificate configuration.

Syntax

```
get system certificate ca [certificate name]
get system certificate crl [crl name]
get system certificate local [certificate name]
get system certificate oftp [certificate name]
get system certificate ssh [certificate name]
```

Example

This example shows the output for `get system certificate local Fortinet_Local`:

```
name : Fortinet_Local
password : *
comment : Default local certificate
private-key :
certificate :
   Subject: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiAnalyzer, CN =
        FAZ-VM0000000001, emailAddress = support@fortinet.com
   Issuer: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority,
        CN = fortinet-subca2001, emailAddress = support@fortinet.com
   Valid from: 2017-08-30 26:03:83 GMT
   Valid to: 2056-01-19 33:14:77 GMT
   Fingerprint: 68:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:7C
   Root CA: No
   Version: 3
   Serial Num:
      38:f9
   Extensions:
      Name: X509v3 Subject Key Identifier
      Critical: no
      Content:
      EC:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:94
      Name: X509v3 Authority Key Identifier
      Critical: no
      Content:
      keyid:98:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:--:D7
```

```
DirName:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate Authority/CN=fortinet-
      ca2/emailAddress=support@fortinet.com
serial:20:01
      Name: X509v3 Basic Constraints
      Critical: yes
      Content:
      CA:FALSE
      Name: X509v3 Key Usage
      Critical: yes
      Content:
      Digital Signature
csr :
```

system dns

Use this command to view DNS settings.

Syntax

```
get system dns
```

Example

This example shows the output for `get system dns`:

```
primary : 111.11.111.11
secondary : 111.11.111.12
ip6-primary : ::
ip6-secondary : ::
```

system fips

Use this command to view FIPS settings.

Syntax

```
get system fips
```

Example

This example shows the output for `get system fips`:

```
entropy-token : enable
re-seed-interval : 1440
```

system fortiview

Use this command to view the FortiView settings.

Syntax

```
get system fortiview auto-cache
get system fortiview settings
```

Example

This example shows the output for `get system fortiview auto-cache`:

```
aggressive-fortiview: disable
interval : 168
status : enable
```

system global

Use this command to view global system settings.

Syntax

```
get system global
```

Example

This example shows the output for `get system global`:

```
admin-https-pki-required: disable
admin-lockout-duration: 60
admin-lockout-threshold: 3
adom-mode : advanced
adom-select : enable
adom-status : enable
backup-compression : normal
backup-to-subfolders: disable
clt-cert-req : disable
console-output : standard
country-flag : enable
create-revision : disable
daylightsavetime : enable
default-disk-quota : 1000
default-search-mode : filter-based
detect-unregistered-log-device: enable
device-view-mode : regular
enc-algorithm : high
fgfm-ssl-protocol : tlsv1.2
```

```
ha-member-auto-grouping: enable
hitcount_concurrent : 100
hitcount_interval : 300
hostname : FAZVM64
language : english
ldap-cache-timeout : 86400
ldapconntimeout : 60000
log-checksum : none
log-mode : analyzer
max-aggregation-tasks: 0
max-running-reports : 1
oftp-ssl-protocol : tlsv1.2
policy-hit-count : disable
policy-object-in-dual-pane: disable
pre-login-banner : disable
remoteauthtimeout : 10
search-all-adoms : disable
ssl-low-encryption : disable
ssl-protocol : tlsv1.2
ssl-static-key-ciphers: enable
task-list-size : 2000
timezone : (GMT-8:00) Pacific Time (US & Canada).
tunnel-mtu : 1500
usg : disable
webservice-proto : tlsv1.2
```

system ha

Use this command to view HA configuration.

Syntax

```
get system ha
```

system interface

Use these commands to view interface configuration and status.

Syntax

```
get system interface
get system interface [interface name]
```

Examples

This example shows the output for `get system interface`:

```
== [ port1 ]
name: port1 status: up ip: 111.11.11.11 255.255.255.0 speed: auto
== [ port2 ]
name: port2 status: up ip: 0.0.0.0 0.0.0.0 speed: auto
== [ port3 ]
name: port3 status: up ip: 0.0.0.0 0.0.0.0 speed: auto
== [ port4 ]
name: port4 status: up ip: 0.0.0.0 0.0.0.0 speed: auto
```

This example shows the output for `get system interface port1`:

```
name : port1
status : up
ip : 111.11.11.11 255.255.255.0
allowaccess : ping https ssh snmp telnet http webservice fgfm
speed : auto
description : (null)
alias : (null)
mtu : 1500
ipv6:
   ip6-address: ::/0 ip6-allowaccess:
```

system locallog

Use these commands to view local log configuration.

Syntax

```
get system locallog disk filter
get system locallog disk setting
get system locallog [fortianalyzer | fortianalyzer2 |fortianalyzer3] filter
get system locallog [fortianalyzer | fortianalyzer2 |fortianalyzer3] setting
get system locallog memory filter
get system locallog memory setting
get system locallog setting
get system locallog [syslogd | syslogd2 | syslogd3] filter
get system locallog [syslogd | syslogd2 | syslogd3] setting
```

Examples

This example shows the output for `get system locallog disk setting`:

```
status : enable
severity : information
upload : disable
server-type : FTP
max-log-file-size : 100
roll-schedule : none
diskfull : overwrite
log-disk-full-percentage: 80
```

This example shows the output for `get system locallog syslogd3 filter`:

```
event : enable
```

```
devops : enable
diskquota : enable
dvm : enable
ediscovery : enable
eventmgmt : enable
faz : enable
fazsys : enable
fmgws : enable
fortiview : enable
hcache : enable
iolog : enable
logd : enable
logdb : enable
logdev : enable
logfile : enable
logging : enable
report : enable
system : enable
```

system log

Use these commands to view log configuration.

Syntax

```
get system log alert
get system log ioc
get system log mail-domain <id>
get system log settings
```

Example

This example shows the output for `get system log settings`:

```
FAC-custom-field1 : (null)
FAZ-custom-field1 : (null)
FCH-custom-field1 : (null)
FCT-custom-field1 : (null)
FDD-custom-field1 : (null)
FGT-custom-field1 : (null)
FMG-custom-field1 : (null)
FML-custom-field1 : (null)
FPX-custom-field1 : (null)
FSA-custom-field1 : (null)
FWB-custom-field1 : (null)
browse-max-logfiles : 10000
dns-resolve-dstip : disable
download-max-logs : 500000
ha-auto-migrate : disable
import-max-logfiles : 10000
log-file-archive-name: basic
rolling-regular:
```

```
sync-search-timeout : 60
```

system log-fetch

Use these commands to view log fetching configuration.

Syntax

```
get system log-fetch client-profile [id]
get system log-fetch server-settings
```

Example

This example shows the output for `get system log-fetch server-settings`:

```
max-conn-per-session: 3
max-sessions : 1
session-timeout : 10
```

system log-forward

Use this command to view log forwarding settings.

Syntax

```
get system log-forward [id]
```

system log-forward-service

Use this command to view log forward service settings.

Syntax

```
get system log-forward-service
```

Example

This example shows the output for `get system log-forward-service`:

```
accept-aggregation : enable
aggregation-disk-quota: 20000
```

system loglimits

Use this command to view log limits on your FortiAnalyzer unit.

Syntax

```
get system loglimits
```

Example

This example shows the output for `get system loglimits`:

```
GB/day : 250
Peak Log Rate : 10000
Sustained Log Rate : 4000
```

Where:

GB/day	Number of gigabytes used per day.
Peak Log Rate	Peak time log rate.
Sustained Log Rate	Average log rate.

system mail

Use this command to view alert email configuration.

Syntax

```
get system mail [mail service id]
```

Example

This example shows the output for an alert email named `Test`:

```
id : Test
auth : disable
passwd : *
port : 25
secure-option : default
server : mailServer
user : mailperson@mailServer.com
```

system metadata

Use this command to view metadata settings.

Syntax

```
get system metadata admins [fieldname]
```

Example

This example shows the output for `get system metadata admins 'Contact Email'`:

```
fieldname : Contact Email
fieldlength : 50
importance : optional
status : enabled
```

system ntp

Use this command to view NTP configuration.

Syntax

```
get system ntp
```

Example

This example shows the output for `get system ntp`:

```
ntpserver:
   == [ 1 ]
   id: 1
status : enable
sync_interval : 60
```

system password-policy

Use this command to view the system password policy.

Syntax

```
get system password-policy
```

Example

This example shows the output for `get system password-policy`:

```
status : enable
minimum-length : 8
must-contain : upper-case-letter lower-case-letter number non-alphanumeric
change-4-characters : disable
expire : 60
```

system performance

Use this command to view performance statistics on your FortiAnalyzer unit.

Syntax

```
get system performance
```

Example

This example shows the output for `get system performance`:

```
CPU:
   Used: 100.00%
   Used(Excluded NICE): 100.00%
         %used %user %nice %sys %idle %iowait %irq %softirq
   CPU0 100.00 100.00 0.00 0.00 0.00 0.00 0.00 0.00
Memory:
   Total: 4,134,728 KB
   Used: 2,105,988 KB 50.9%
Hard Disk:
   Total: 82,434,456 KB
   Used: 3,836,324 KB 4.7%
   IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
           1.4 0.1 1.4 1.3 22.8 0.0 4.8 2.4 0.3 448240.73
Flash Disk:
   Total: 499,656 KB
   Used: 112,312 KB 22.5%
   IOStat: tps r_tps w_tps r_kB/s w_kB/s queue wait_ms svc_ms %util sampling_sec
           0.0 0.0 0.0 0.0 0.0 0.0 2.8 0.9 0.0 448240.82
```

system report

Use this command to view report configuration.

Syntax

```
get system report auto-cache
get system report est-browse-time
get system report group [group id]
get system report setting
```

Example

This example shows the output for `get system report setting`:

```
aggregate-report : disable
ldap-cache-timeout : 60
max-table-rows : 10000
report-priority : auto
template-auto-install: default
week-start : sun
```

system route

Use this command to view IPv4 routing table configuration.

Syntax

```
get system route [seq_num]
```

Example

This example shows the output for `get system route 66`:

```
seq_num : 66
device : port5
dst : 0.0.0.0 0.0.0.0
gateway : 10.111.1.16
```

system route6

Use this command to view IPv6 routing table configuration.

Syntax

```
get system route6 [seq_num]
```

system snmp

Use these commands to view SNMP configuration.

Syntax

```
get system snmp community [community ID]
get system snmp sysinfo
get system snmp user [SNMP user name]
```

Example

This example shows the output for `get system snmp sysinfo`:

```
contact_info : (null)
description : Test FAZ
engine-id : (null)
fortianalyzer-legacy-sysoid: disable
location : (null)
status : enable
trap-cpu-high-exclude-nice-threshold: 80
trap-high-cpu-threshold: 80
trap-low-memory-threshold: 80
```

system sql

Use this command to view SQL configuration.

Syntax

```
get system sql
```

Example

This example shows the output for `get system sql`:

```
custom-index:
prompt-sql-upgrade : enable
status : local
text-search-index : disable
ts-index-field:
   == [ FGT-app-ctrl ]
   category: FGT-app-ctrl value: user,group,srcip,dstip,dstport,service,app,action,hostname
   == [ FGT-attack ]
   category: FGT-attack value: severity,srcip,dstip,action,user,attack
   == [ FGT-content ]
   category: FGT-content value: from,to,subject,action,srcip,dstip,hostname,status
   == [ FGT-dlp ]
```

```
    category: FGT-dlp value: user,srcip,service,action,filename
    == [ FGT-emailfilter ]
    category: FGT-emailfilter value: user,srcip,from,to,subject
    == [ FGT-event ]
    category: FGT-event value: subtype,ui,action,msg
    == [ FGT-traffic ]
    category: FGT-traffic value: user,srcip,dstip,service,app,utmaction
    == [ FGT-virus ]
    category: FGT-virus value: service,srcip,dstip,action,filename,virus,user
    == [ FGT-voip ]
    category: FGT-voip value: action,user,src,dst,from,to
    == [ FGT-webfilter ]
    category: FGT-webfilter value: user,srcip,dstip,service,action,catdesc,hostname
    == [ FGT-netscan ]
    category: FGT-netscan value: user,dstip,vuln,severity,os
    == [ FGT-fct-event ]
    category: FGT-fct-event value: (null)
    == [ FGT-fct-traffic ]
    category: FGT-fct-traffic value: (null)
    == [ FGT-fct-netscan ]
    category: FGT-fct-netscan value: (null)
    == [ FGT-waf ]
    category: FGT-waf value: user,srcip,dstip,service,action
    == [ FGT-gtp ]
    category: FGT-gtp value: msisdn,from,to,status
    == [ FGT-dns ]
    category: FGT-dns value: (null)
    == [ FGT-ssh ]
    category: FGT-ssh value: (null)
    == [ FML-emailfilter ]
    category: FML-emailfilter value: client_name,dst_ip,from,to,subject
    == [ FML-event ]
    category: FML-event value: subtype,msg
    == [ FML-history ]
    category: FML-history value: classifier,disposition,from,to,client_
         name,direction,domain,virus
    == [ FML-virus ]
    category: FML-virus value: src,msg,from,to
    == [ FWB-attack ]
    category: FWB-attack value: http_host,http_url,src,dst,msg,action
    == [ FWB-event ]
    category: FWB-event value: ui,action,msg
    == [ FWB-traffic ]
    category: FWB-traffic value: src,dst,service,http_method,msg
background-rebuild : enable
database-type : postgres
device-count-high : disable
event-table-partition-time: 0
fct-table-partition-time: 240
rebuild-event : enable
rebuild-event-start-time: 00:00 2000/01/01
start-time : 00:00 2000/01/01
traffic-table-partition-time: 0
utm-table-partition-time: 0
```

system status

Use this command to view the status of your FortiAnalyzer unit.

Syntax

```
get system status
```

Example

This example shows the output for `get system status`:

```
Platform Type : FAZ3000D
Platform Full Name : FortiAnalyzer-3000D
Version : v6.0.1-build0150 180606 (GA)
Serial Number : F--------------2
BIOS version : 00010005
System Part-Number : P12907-03
Hostname : FAZ3000D
Max Number of Admin Domains : 4000
Admin Domain Configuration : Enabled
FIPS Mode : Disabled
Branch Point : 0150
Release Version Information : GA
Current Time : Tue Sep 29 08:09:05 PDT 2020
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
x86-64 Applications : Yes
Disk Usage : Free 3083.01GB, Total 7332.97GB
File System : Ext4
```

system syslog

Use this command to view syslog information.

Syntax

```
get system syslog [syslog server name]
```

Example

This example shows the output for an syslog server named `Test`:

```
name : Test
ip : 10.10.10.1
port : 514
```

system workflow

Use this command to view workflow approval matrix information.

Syntax

```
get system workflow approval-matrix [adom]
```

show

The `show` commands display a part of your unit's configuration in the form of the commands that are required to achieve that configuration from the firmware's default state.

Although not explicitly shown in this section, for all `config` commands, there are related `show` commands that display that part of the configuration. The `show` commands use the same syntax as their related `config` command.

CLI commands and variables are case sensitive.

Unlike the `get` command, `show` does not display settings that are in their default state.

Example

```
FAZVM64 # show system global
   config system global
      set adom-mode advanced
      set adom-status enable
      set hostname "FAZVM64"
   end
```

Appendix A - Object Tables

Global object categories

38 "webfilter ftgd-local-cat"	47 "webfilter urlfilter"	51 "webfilter ftgd-local-rating"
52 "vpn certificate ca"	56 "spamfilter bword"	60 "spamfilter dnsbl"
64 "spamfilter mheader"	67 "spamfilter iptrust"	85 "ips custom"
140 "firewall address"	142 "firewall addrgrp"	255 "user adgrp"
145 "user radius"	146 "user ldap"	147 "user local"
148 "user peer"	152 "user group"	167 "firewall service custom"
254 "firewall service predefined"	168 "firewall service group"	170 "firewall schedule onetime"
171 "firewall schedule recurring"	172 "firewall ippool"	173 "firewall vip"
288 "ips sensor"	292 "log custom-field"	293 "user tacacs+"
296 "firewall ldb-monitor"	1028 "application list"	1038 "dlp sensor"
1043 "wanopt peer"	1044 "wanopt auth-group"	1054 "vpn ssl web portal"
1076 "system replacemsg-group"	1097 "firewall mms-profile"	1203 "firewall gtp"
1213 "firewall carrier-endpoint-bwl"	1216 "antivirus notification"	1327 "webfilter content"
1337 "endpoint-control profile"	1338 "firewall schedule group"	1364 "firewall shaper traffic-shaper"
1365 "firewall shaper per-ip-shaper"	1367 "vpn ssl web virtual-desktop-app-list"	1370 "vpn ssl web host-check-software"
1413 "webfilter profile"	1420 "antivirus profile"	1433 "spamfilter profile"
1472 "antivirus mms-checksum"	1482 "voip profile"	150 "system object-tag"
184 "user fortitoken"	273 "web-proxy forward-server"	335 "dlp filepattern"
343 "icap server"	344 "icap profile"	321 "user fsso"
390 "system sms-server"	397 "spamfilter bwl"	457 "wanopt profile"
384 "firewall service category"	474 "application custom"	475 "user device-category"
476 "user device"	492 "firewall deep-inspection-options"	800 "dynamic interface"
810 "dynamic address"	1004 "vpnmgr vpntable"	1005 "vpnmgr node"
1100 "system meta"	820 "report output"	822 "sql-report chart"
824 "sql-report dataset"	825 "sql-report dashboard"	827 "sql-report layout"

1494 "dynamic vip"	1495 "dynamic ippool"	1504 "dynamic certificate local"
1509 "dynamic vpntunnel"		

Device object ID values

1 "system vdom"	3 "system accprofile"	5 "system admin"
8 "system interface"	16 "system replacemsg mail"	17 "system replacemsg http"
18 "system replacemsg ftp"	19 "system replacemsg nntp"	20 "system replacemsg alertmail"
21 "system replacemsg fortiguard-wf"	22 "system replacemsg spam"	23 "system replacemsg admin"
24 "system replacemsg auth"	25 "system replacemsg im"	26 "system replacemsg sslvpn"
28 "system snmp community"	38 "webfilter ftgd-local-cat"	1300 "application recognition predefined"
47 "webfilter urlfilter"	51 "webfilter ftgd-local-rating"	52 "vpn certificate ca"
53 "vpn certificate local"	54 "vpn certificate crl"	55 "vpn certificate remote"
56 "spamfilter bword"	60 "spamfilter dnsbl"	64 "spamfilter mheader"
67 "spamfilter iptrust"	74 "imp2p aim-user"	75 "imp2p icq-user"
76 "imp2p msn-user"	77 "imp2p yahoo-user"	85 "ips custom"
117 "system session-helper"	118 "system tos-based-priority"	124 "antivirus service"
128 "antivirus quarfilepattern"	130 "system ipv6-tunnel"	314 "system sit-tunnel"
131 "system gre-tunnel"	132 "system arp-table"	135 "system dhcp server"
137 "system dhcp reserved-address"	138 "system zone"	140 "firewall address"
142 "firewall addrgrp"	255 "user adgrp"	145 "user radius"
146 "user ldap"	147 "user local"	148 "user peer"
152 "user group"	155 "vpn ipsec phase1"	156 "vpn ipsec phase2"
157 "vpn ipsec manualkey"	158 "vpn ipsec concentrator"	165 "vpn ipsec forticlient"
167 "firewall service custom"	254 "firewall service predefined"	168 "firewall service group"
170 "firewall schedule onetime"	171 "firewall schedule recurring"	172 "firewall ippool"
173 "firewall vip"	178 "firewall ipmacbinding table"	181 "firewall policy"
189 "firewall dnstranslation"	190 "firewall multicast-policy"	199 "system mac-address-table"
200 "router access-list"	202 "router aspath-list"	204 "router prefix-list"
206 "router key-chain"	208 "router community-list"	210 "router route-map"

225 "router static"	226 "router policy"	253 "system proxy-arp"
284 "system switch-interface"	285 "system session-sync"	288 "ips sensor"
292 "log custom-field"	293 "user tacacs+"	296 "firewall ldb-monitor"
297 "ips decoder"	299 "ips rule"	307 "router auth-path"
317 "system wccp"	318 "firewall interface-policy"	1020 "system replacemsg ec"
1021 "system replacemsg nac-quar"	1022 "system snmp user"	1027 "application name"
1028 "application list"	1038 "dlp sensor"	1041 "user ban"
1043 "wanopt peer"	1044 "wanopt auth-group"	1045 "wanopt ssl-server"
1047 "wanopt storage"	1054 "vpn ssl web portal"	1061 "system wireless ap-status"
1075 "system replacemsg-image"	1076 "system replacemsg-group"	1092 "system replacemsg mms"
1093 "system replacemsg mm1"	1094 "system replacemsg mm3"	1095 "system replacemsg mm4"
1096 "system replacemsg mm7"	1097 "firewall mms-profile"	1203 "firewall gtp"
1213 "firewall carrier-endpoint-bwl"	1216 "antivirus notification"	1326 "system replacemsg traffic-quota"
1327 "webfilter content"	1337 "endpoint-control profile"	1338 "firewall schedule group"
1364 "firewall shaper traffic-shaper"	1365 "firewall shaper per-ip-shaper"	1367 "vpn ssl web virtual-desktop-app-list"
1370 "vpn ssl web host-check-software"	1373 "report dataset"	1375 "report chart"
1382 "report summary"	1387 "firewall sniff-interface-policy"	1396 "wireless-controller vap"
1399 "wireless-controller wtp"	1402 "wireless-controller ap-status"	1412 "system replacemsg webproxy"
1413 "webfilter profile"	1420 "antivirus profile"	1433 "spamfilter profile"
1440 "firewall profile-protocol-options"	1453 "firewall profile-group"	1461 "system storage"
1462 "report style"	1463 "report layout"	1472 "antivirus mms-checksum"
1482 "voip profile"	1485 "netscan assets"	1487 "firewall central-nat"
1490 "report theme"	150 "system object-tag"	169 "system dhcp6 server"
180 "system port-pair"	182 "system 3g-modem custom"	183 "application rule-settings"
184 "user fortitoken"	212 "webfilter override"	270 "firewall local-in-policy"
273 "web-proxy forward-server"	330 "system ddns"	331 "system replacemsg captive-portal-dflt"
335 "dlp filepattern"	337 "dlp fp-sensitivity"	338 "dlp fp-doc-source"
342 "webfilter ftgd-warning"	343 "icap server"	344 "icap profile"

352 "system monitors"	354 "system sp"	321 "user fsso"
355 "router gwdetect"	386 "system physical-switch"	388 "system virtual-switch"
390 "system sms-server"	394 "system replacemsg utm"	397 "spamfilter bwl"
406 "vpn certificate ocsp-server"	408 "user password-policy"	412 "webfilter search-engine"
428 "firewall identity-based-route"	431 "web-proxy debug-url"	432 "firewall ttl-policy"
434 "firewall isf-acl"	435 "firewall DoS-policy"	437 "firewall sniffer"
438 "wireless-controller wids-profile"	439 "switch-controller vlan"	441 "switch-controller managed-switch"
453 "firewall ip-translation"	457 "wanopt profile"	269 "firewall multicast-address"
384 "firewall service category"	466 "system ips-urlfilter-dns"	467 "system geoip-override"
474 "application custom"	475 "user device-category"	476 "user device"
483 "system server-probe"	473 "system replacemsg device-detection-portal"	492 "firewall deep-inspection-options"

Appendix B - CLI Error Codes

Some FortiAnalyzer CLI commands issue numerical error codes. The following table lists the error codes and descriptions.

Error Code	Description
0	Success
1	Function called with illegal parameters
2	Unknown protocol
3	Failed to connect host
4	Memory failure
5	Session failure
6	Authentication failure
7	Generic file transfer failure
8	Failed to access local file
9	Failed to access remote file
10	Failed to read local file
11	Failed to write local file
12	Failed to read remote file
13	Failed to write remote file
14	Local directory failure
15	Remote directory failure